

ATTENTION

The following documents appearing in FBI files have been reviewed under the provisions of The Freedom of Information Act (FOIA) (Title 5, United States Code, Section 552); Privacy Act of 1974 (PA) (Title 5, United States Code, Section 552a); and/or Litigation.

☐ FOIA/PA☐ Litigation☐ Executive Order Applied

Requester: _____

Subject: _____

Computer or Case Identification Number: _____

Title of Case: _____ Section _____

* File _____

Serials Reviewed: _____

Release Location: *File _____ Section _____

This file section has been scanned into the FOIPA Document Processing System (FDPS) prior to National Security Classification review. Please see the documents located in the FDPS for current classification action, if warranted. Direct inquiries about the FDPS to RIDS Service Request Unit, 202-324- b2

File Number: 288A-SF-133411 Section 1Serial(s) Reviewed: ALL

FOIPA Requester: _____

FOIPA Subject: _____

FOIPA Computer Number: 991994

File Number: _____ Section _____

Serial(s) Reviewed: _____

FOIPA Requester: _____

FOIPA Subject: _____

FOIPA Computer Number: _____

File Number: _____ Section _____

Serial(s) Reviewed: _____

FOIPA Requester: _____

FOIPA Subject: _____

FOIPA Computer Number: _____

THIS FORM IS TO BE MAINTAINED AS THE TOP SERIAL OF THE FILE, BUT NOT SERIALIZED.

ATTENTION

DO NOT REMOVE FROM FILE

(12/31/95)

FEDERAL BUREAU OF INVESTIGATION

Precedence: ROUTINE

Date: 01/03/2003

To: Cyber

Attn: CCIU

From: San Francisco
14B

Contact:

Approved By:

b7C

Drafted By:

Case ID # 288A-SF-new 133411/1

Title: UNSUB(S);
GOOGLE - VICTIM--VICTIM
SUNNYVALE, CA
NIPC - Impairment
01/02/2003

SUBMISSION: ☒ Initial ☐ Supplemental ☐ Closing

Case Opened: 01/03/2003

Case Closed:

- ☐ No Action Due to State/Local Prosecution (Name/Number)
- ☐ USA Declination
- ☐ Referred to Another Federal Agency (Name/Number)
- ☐ Placed In Unaddressed work
- ☐ Closed Administratively
- ☐ Conviction

COORDINATION: FBI Field Office San Francisco
Government Agency _____
Private Corporation _____

VICTIM

b7C

Company name/Government agency GOOGLE - VICTIM
Address/location: SUNNYVALE, CA

Purpose of System: SEARCH ENGINE
Highest classification of information stored in system: ☒ Unclas ☐ Confidential
☐ Secret ☐ Top Secret

*Router
08A-288A-new
TO
1/3-03*

288A-SF-133411

To: Counterterrorism, FBI From: San Francisco
Re: 288A-SF-new

Date 01/03/2003

System Data:

Hardware/configuration (CPU) _____
Operating System: _____
Software _____

Security Features:

Security Software Installed: ☐ Yes (identify _____) ☒ NO
Logon Warning Banner: ☒ Yes ☐ No

INTRUSION INFORMATION

Access for intrusion: ☒ Internet connection ☐ dial-up number ☐ LAN (insider)
If Internet: Internet Address: _____
Network Name: GOOGLE.COM

Method:

Technique(s) used in intrusion: UDP Flooding
PING Flooding
SYN Flood

Path of intrusion:

Addresses	Country:	Facility:
1 _____	1 _____	1 _____
2 _____	2 _____	2 _____
3 _____	3 _____	3 _____
4 _____	4 _____	4 _____
5 _____	5 _____	5 _____

Subject:

Age _____ Race: _____
Sex _____ Education: _____
Alias(s): _____ Motive: _____
Group Affiliation: _____
Employer: _____
Known Accomplices: _____
Equipment used: _____
Hardware/configuration (CPU) _____
Operating System: _____
Software: _____

Impact:

Compromise of classified information: ☐ Yes ☒ no
Estimated Number of Computers effected: _____ 2
Estimated Dollar loss to date total: _____ \$5,000.00

To: Counterterrorism
Re: 288A-SF-new

From: San Francisco

Date 01-03-2003

Category of Crime:

Impairment:

- ☐ Malicious code inserted
- ☒ Denial of Service
- ☐ Destruction of information/software
- ☐ Modification of information/software

Intrusion:

- ☐ Unauthorized access
- ☐ Exceeding authorized access

Theft of Information:

- ☐ Classified information compromised
- ☐ Unclassified information compromise
- ☐ Passwords obtained
- ☐ Computer processing time obtained
- ☐ Telephone services obtained
- ☐ Application software obtained
- ☐ Operating software obtained

REMARKS

On 1/2/2002, two DoS were launched against Google.com. The first attack was at approximately 4:00a, lasting approximately 5-7 minutes, affecting servers in Santa Clara. The second attack occurred at approximately 3:00p PST, lasting approximately 5-7 minutes, affecting servers in both Santa Clara and Virginia.

FEDERAL BUREAU OF INVESTIGATION

Precedence: IMMEDIATE

Date: 01/03/2003

To: Chicago

From: San Francisco

14B/HRA

Contact: SA [REDACTED]

Approved By: [REDACTED] M

Drafted By: [REDACTED] am Am

Case ID #: 288A-SF-133411 - (Pending)

Title: UNSUB(S);
GOOGLE - VICTIM
SUNNYVALE, CA
NIPC - Impairment

Synopsis: To set lead to Chicago to interview [REDACTED]
[REDACTED] e-mail [REDACTED] telephone number [REDACTED]
fax number [REDACTED] website [REDACTED]

Details: Google.com was a victim of two Denial of Service (DOS) attacks on January 2, 2003. The first attack occurred around 4:00 A.M. PST, lasting approximately five to seven minutes, and affected Google.com's Santa Clara servers. The second attack occurred around 3:00 P.M. PST, lasting approximately five to seven minutes, and affected both Google.com's Santa Clara and Virginia servers. The first attack was a DOS attack comprised of both UDP and Ping Flood attacks. The second attack was on a much larger scale and consisted of a SYN Flood attack.

[REDACTED] Google.com security, was advised of the first attack by [REDACTED] is a member of the Forum of Incident Response and Security Teams (FIRST.) [REDACTED] called [REDACTED] around 8:00 A.M. PST to advise him that a reconnaissance bot of [REDACTED] had detected an attack on Google.com. [REDACTED] verified in the server logs that such an attack did take place.

[REDACTED] believes an individual, who goes by the Internet Relay Chat (IRC) name of [REDACTED] may be responsible for the attacks. This name was found by [REDACTED] from server log entries. [REDACTED] at one point had an affiliation with Global Threat (GT), a hacking group.

San Francisco Division requests Chicago Division locate and interview [REDACTED]

288A-SF-133411-2

To: Chicago From: San Francisco
Re: 288A-SF-133411, 01/03/2003

LEAD(s):

Set Lead 1:

CHICAGO

AT CHICAGO, IL

b7C

Please locate and interview [redacted] e-mail
[redacted] telephone number [redacted] fax number [redacted]
[redacted] website [redacted] concerning the DOS attacks
against Google.com as referenced above. Please collect pertinent
log files and other electronic evidence and forward to writer.

♦♦

- 1 -

FEDERAL BUREAU OF INVESTIGATION

Date of transcription 01/03/2003

[redacted] an employee of GOOGLE.COM, cell phone number [redacted] work phone number [redacted] was interviewed on January 3, 2003. Also present was [redacted] GOOGLE.COM general counsel, cell phone number [redacted] office phone number [redacted]. After being advised of the identities of the Agents and the nature of the interview, [redacted] provided the following information:

GOOGLE.COM, an internet search engine host, was attacked by two separate Denial of Service (DOS) attacks on January 2, 2003. The first attack occurred around 4:00 A.M. PST. This attack lasted approximately five to seven minutes and was a combination of both UDP and Ping Flood attacks. [redacted] was made aware of the first attack by [redacted] a member of the FORUM OF INCIDENT RESPONSE AND SECURITY TEAMS (FIRST), first discovered the attack through a "reconnaissance bot" he has installed. [redacted] called and asked [redacted] if GOOGLE.COM experienced a DOS attack sometime in the early morning of January 2, 2003. [redacted] verified in the server logs that such an attack did take place. [redacted] estimates that this first DOS attack came from roughly 4,000 hosts. This attack targeted the Santa Clara server farm of GOOGLE.COM.

The second DOS attack on GOOGLE.COM occurred around 3:00 P.M. PST. This attack was on a much larger scale, also lasting five to seven minutes, and was a SYN Flood attack. This attack had a more global affect on GOOGLE.COM's network, affecting servers in Santa Clara and Virginia, causing roughly one of every three searches a user submitted to fail. [redacted] called [redacted] to see if he had also detected this attack. [redacted] missed the attack due to a failed server. When the server restarted the attack had already ceased.

GOOGLE.COM does not come under this level of attack very often, therefore [redacted] believes that both attacks were executed by the same person. [redacted] told [redacted] that [redacted] an Internet Relay Chat (IRC) name, may be responsible for the attacks. [redacted] gained this information from the log files from IRC channel traffic being monitored by [redacted]. The log files showed that [redacted] had launched commands, similar to those that launched the attack on GOOGLE.COM, from a DALNET IRC server. [redacted] is known to frequently use the

Investigation on 1/3/2003 at Hayward, California (telephonically)File # 288A-SF-133411 - 3 b7C Date dictated

by SA [redacted] " [redacted] : [redacted] GOOGLE 01.302" ✓

288A SF 133411 - 3

288A-SF-133411

b7C

b7D

Continuation of FD-302 of

[Redacted]

, On 1/3/2003

, Page 2

DALNET servers for the purpose of commanding bots. [Redacted] was, at one point, affiliated with GLOBAL THREAT (GT), an organization known for creating bots.

b7C

14B

- 1 -

FEDERAL BUREAU OF INVESTIGATION

Date of transcription 01/13/2003

On January 13, 2003. Source who is not in the position to testify contacted SA [redacted] via e-mail. The body of the e-mail contained, in part, the following:

b7C

Hey [redacted]
Happy new year to you too.
this one I can actually help you with [redacted] but the network got split
up and everyone pretty much left. I'm not sure where they are located right now, but I could probably find out. I

b7C

b7D

[redacted]
[redacted] is also in the log file.
and I have seen [redacted] around I just don't any information on them.

I've attached the log file.

Also I'm free for lunch pretty much anytime next week. I'll give you a ring say Monday?

The log file mentioned above was attached to the e-mail received and was named [redacted]. An electronic copy of this file was written to floppy disk and is contained in the 1A portion of both case files.

b7D

L: [redacted] 017aws01.wpd

b7C

Investigation on 01/13/2003 at Hayward, Ca

File # 288A-SF-133411

Date dictated Not Dictated

by SA [redacted]:aws

b2

b7D

This document contains neither recommendations nor conclusions of the FBI. It is the property of the FBI and is loaned to your agency; it and its contents are not to be distributed outside your agency.

288A-SF-133411-4

- 1 -

FEDERAL BUREAU OF INVESTIGATION

Date of transcription 01/10/2003

On January 10, 2003, Source who is not in the position b7C
to testify was electronically contacted via e-mail by SA
 The body of the e-mail contained the following:

Happy New Year. Hope all is well and things are going well with your new business venture.

I was wondering if you had information regarding the following:

b7D Channel:

Nicks:

b7C

Names:

b7D Website:

Anything concerning DDOS attacks against Google and DALNET.

Anything about commands being run on/through DALNET and Bots locations.

Give me a call some time soon so we can get together for lunch/coffee.

Take Care,

b7C

Investigation on 01/10/2003 at Hayward, Ca

File # 288A-SF-133411 SubA ^{b2} Date dictated Not Dictated

by SA :aws *[Signature]*

b7D

b7C

This document contains neither recommendations nor conclusions of the FBI. It is the property of the FBI and is loaned to your agency; it and its contents are not to be distributed outside your agency.

288A-SF-133411-5

- 1 -

FEDERAL BUREAU OF INVESTIGATION

Date of transcription 01/16/2003

On January 15, 2003, SA [redacted] Federal Bureau of Investigation, San Francisco Division, Hayward Resident Agency, conducted the following investigation: b7C

I performed an Internet search of the website [redacted] and discovered the following: the website address [redacted] is owned by the same person as the website address [redacted]. The site shows [redacted] as the individual who owns maintains the site [redacted] is the first person registered on the message forum. b2 b7C

b7C

Investigation on 1-15-2003 at Hayward, California

File # 288A-SF-133411 -6 Date dictated Not Dictated

by SA [redacted] b7C

This document contains neither recommendations nor conclusions of the FBI. It is the property of the FBI and is loaned to your agency; it and its contents are not to be distributed outside your agency.

SEE 1A(2)

288A-SF-133411-6

- 1 -

FEDERAL BUREAU OF INVESTIGATION

Date of transcription 01/16/2003

On January 13, 2003, SA [redacted] Federal Bureau of Investigation, San Francisco Division, Hayward Resident Agency, conducted the following investigation: b7C

I performed an open source Internet database check on the Internet address, [redacted]. This Internet address (url) is registered to [redacted] telephone number [redacted] e-mail address [redacted] b2 b7C

b7C

Investigation on 1-13-2003 at Hayward, CaliforniaFile # 288A-SF-133411-1 Date dictated Not Dictatedby SA [redacted] b7C

This document contains neither recommendations nor conclusions of the FBI. It is the property of the FBI and is loaned to your agency; it and its contents are not to be distributed outside your agency.

288A-SF-133411-7

- 1 -

FEDERAL BUREAU OF INVESTIGATION

Date of transcription 01/16/2003

[redacted] an employee of GOOGLE.COM, work address 2400 Bayshore Parkway, Mountain View, California, 94043, cell phone number [redacted] work phone number [redacted] e-mail address [redacted] was interviewed on January 7, 2003. After being advised of the identity of the Agent and the nature of the interview, [redacted] provided the following information:

[redacted] reviewed logs from GOOGLE.COM's servers. The logs were unclear as to whom launched the January 2, 2003, Denial of Service attacks against GOOGLE.COM. b7C

[redacted] is working with [redacted] on finalizing GOOGLE.COM's loss estimate.

[redacted] has been with GOOGLE.COM [redacted] Information Security Officer. Before working at GOOGLE.COM, [redacted] was employed at [redacted] for many years.

b7C

Investigation on 1-16-2003 at Hayward, California (telephonically)

File # 288A-SF-133411 - 8 Date dictated Not Dictated

by SA [redacted] b7C

- 1 -

FEDERAL BUREAU OF INVESTIGATION

Date of transcription 01/16/2003

On January 13, 2003, SA [redacted] Federal Bureau of Investigation, San Francisco Division, Hayward Resident Agency, conducted the following investigation:

b7C

I performed an open source Internet database check on the Internet address, [redacted] This Internet address (url) is registered to [redacted] [redacted] telephone number [redacted] e-mail address [redacted]

b2

b7C

An

b7C

✓ "C" [redacted] 302

Investigation on 1-13-2003 at Hayward, CaliforniaFile # 288A-SF-133411-9 Date dictated Not Dictated

by SA [redacted] b7C

SEE 1A (5)

288A-SF-133411-9

- 1 -

FEDERAL BUREAU OF INVESTIGATION

Date of transcription 01/16/2003

On January 8, 2003, 4:20 P.M., SA [redacted] received an e-mail from [redacted] Information Security Officer, Google, Inc. The email is attached below:

To: nccs-sf@fbi.gov
cc :
Date: Wed, January 08, 2003, 16:20:00
Subject: Interesting URLs
Date: Wed, January 08, 2003, 16:20:00
Subject: Interesting URLs

b7C

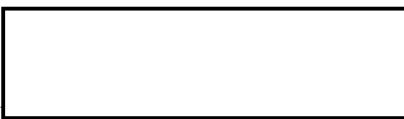
(1,2)
Am

Attention Agent [redacted]

Agent [redacted]

As I promised in our earlier phone conversation, here are a few web pages that seem to refer to [redacted] or his associates. I'm afraid that they don't look particularly promising.

b7C



However, one of our engineers, through a friend-of-a-friend sort of chain, came up with a name, address, and phone number for [redacted]

b7C



I have a meeting tomorrow evening to discuss what information in our logs we can provide. I'll contact you on Friday about this.

b7C

Investigation on 1-16-2003 at Hayward, California

File # 288A-SF-133411 ¹⁰ Date dictated Not Dictated

by SA [redacted] b7C

This document contains neither recommendations nor conclusions of the FBI. It is the property of the FBI and is loaned to your agency; it and its contents are not to be distributed outside your agency.

SEE 1A(6)

288A-SF-133411-10

288A-SF-133411

Continuation of FD-302 of _____, On 1-16-2003, Page 2

Sincerely,

[Redacted Signature]

#+

[Redacted] Information Security Officer [Redacted]

Google, Inc. 2400 Bayshore Parkway, Mountain View, CA 94043

Phone [Redacted] Fax [Redacted]

b7C

- 1 -

FEDERAL BUREAU OF INVESTIGATION

Date of transcription 01/16/2003

On January 16, 2003, 12:02 P.M., SA [redacted] received an e-mail from [redacted] NCC Security Response Team, Fish and Wildlife Services, work telephone number [redacted]. The email is attached below:

b7C

From: [redacted]

To: nccs-sf@fbi.gov

cc: [redacted]

Date: Thu, January 16, 2003, 12:02:00

Subject: Attention- Agent [redacted]

(FWS [redacted] incident 01/06/03)

b7C

b7C

Below are the incident notes I took for the [redacted] found on the [redacted] machine administered by [redacted] Waubay National Wildlife Refuge.

I'm making a copy of the Ghosted image to send you right now. Let me know if you need anything else.

b2

b7C

[redacted]
NCC Security Response Team

NOTES:

1/6/03 9am

Called FBI agent [redacted] (Chicago) back regarding voice mail (8am) he left [redacted]

Notes from FBI conversation:

FBI Case#288a-sf-13341 out of San Fran

b7C

Victim IP [redacted]

b2

Expoit- Open shares bot affecting [redacted] machines without admin, passwords

IP first joined IRC channel on Jan3rd, 2003, 8:14:29pm

b7C

GMT (1:14:29 MST), look in logs for IP aquired around

Investigation on 1-16-2003 at Hayward, CaliforniaFile # 288A-SF-133411-11Date dictated Not Dictated

by SA [redacted] b7C

92E 1A(7)

288A-SF-133411-11

288A-SF-133411

Continuation of FD-302 of _____, On 1-16-2003, Page 2

that time

Check for listening on ports [redacted] and talking on [redacted]

b2

Possibly being used as an attack platform in a DDOS network.

b7C

I sent note to [redacted] regarding event as FYI.

Called [redacted] and left voice mail regarding event.

Went through [redacted] logs and found IP assigned to userid [redacted] during that time.

b7C

Copies of relevent log events:

Jan-03-2003 13:13:29 Accounting start record for user [redacted]

b2

[redacted] start_time=1041624777, timezone=MST, service=ppp

b7C

Jan-03-2003 13:47:40 Accounting stop record for user [redacted]

[redacted] start_time=1041624777, timezone=MST, service=ppp, protocol=ip, addr [redacted]

b7C

Filled out Incident Response Form and sent to [redacted]

[redacted] and CC:ed [redacted]

[redacted] for her to make initial contact with [redacted] to brief him on the incident.

b7C

Called [redacted] FBI, to inform him we found the victim and recieved directions from him on what to look for, ie, [redacted]

Called [redacted] and informed him that his machine has been hacked and gave him

288A-SF-133411

Continuation of FD-302 of _____

, On 1-16-2003 , Page 3

directions to back-up his sensitive data and send machine (just the box) to me at the NCC in Denver. I requested he do nothing to any other files except back up his important ones and that we need the machine for further forensic analysis and will have it for an estimated 4 weeks.

1/8/03

7am- Sent note to [redacted] informing him we should be getting the box this week.

b7C

10am Recieved the box:

Gateway E Series, WIN2k-SP3

Intel P4, 2.0 GHz, 524 Megs RAM

Computer name [redacted]

no modem (must be external, I called and confirmed attached to an external modem)

no admin password

NO mirc.ini file (been removed by [redacted])

b7C

Malware files -

C:\WINNT\system32\dhcp\

file created/modified

12/26/2002 8:55PM (Pacific Time)

12/26/2002 8:55PM (Pacific Time)

12/26/2002 8:55PM (Pacific Time)

12/26/2002 8:55PM (Pacific Time)

12/26/2002 8:56PM (Pacific Time)

12/26/2002 8:57PM (Pacific Time)

1/6/2002 2:06PM(Pacific Time)

1/7/2002 7:12PM(Pacific Time)

1/7/2002 7:12PM(Pacific Time)

1/8/2002 3:42PM(Pacific Time)

b2

C:\WINNT\system32\Microsoft\Crypto\RSA\S-1-5-18\

change.txt 11/14/2002 1:48PM(Pacific Time)

text.txt 11/14/2002 1:49PM(Pacific Time)

C:\WINNT\system32\Microsoft\Crypto\RSA\S-1-5-18\1\

-[MKZ] - 200 11/18/2002 2:49PM(Pacific Time)

- 0.5 mb 11/22/2002 12:05PM(Pacific

Time)

--[55 kb]-- 11/22/2002 12:43PM(Pacific Time)

288A-SF-133411

Continuation of FD-302 of _____, On 1-16-2003, Page 4

C:\WINNT\system32\Microsoft\Crypto\RSA\S-1-5-18\Serv-U\

[redacted] ni 11/17/2002 2:54PM(Pacific Time)
[redacted] xt- 11/17/2002 2:56PM(Pacific
Time)
[redacted] exe 11/17/2002 2:47PM(Pacific
Time)

b2

Malware services running:

[redacted] Service: ir Automatic
Serv-U FTP Server Automatic

Website explaining the attack in detail

-http://www.[redacted].html

1/9 - Called [redacted] back at FBI and he said
someone from San Fran office will be calling me about
the box.

b7C

1/10 - Ghosted image to network. 1.9 gigs.

1/13- Burned image to 3 CDs and removed image from
network server. I had [redacted] re-image machine with
WIN2000 Pro and give it an admin password. Will send
machine back to [redacted] when re-image is complete.

b7C

1/16- Sent box back to [redacted] in South Dakota

b7C

- 1 -

FEDERAL BUREAU OF INVESTIGATION

Date of transcription 01/16/2003

On January 15, 2003, SA [redacted] Federal Bureau of Investigation, San Francisco Division, Hayward Resident Agency, conducted the following investigation:

b7C

I performed an Internet search of the website [redacted] and discovered the following: [redacted] has a staff consisting of the nickname (nic) [redacted] telephone number [redacted] e-mail addresses [redacted] and [redacted]

b7C

The Internet Relay Chat (IRC) [redacted] may be used for contact for each individual on the [redacted] channel on [redacted] IRC servers. The website [redacted] is owned and maintained by [redacted]

①
A7

b7C

✓ "011" [redacted] 302

Investigation on 1-15-2003 at Hayward, CaliforniaFile # 288A-SF-133411-12 Date dictated Not Dictatedby SA [redacted] b7C

See 1A(8)

288A-SF-133411-12

288A-SF-133411
AM:am

13

1

On January 14, 2003, SA [redacted] Federal Bureau of Investigation, San Francisco Division, Hayward Resident Agency, conducted the following investigation:

b7C

I performed an open source Internet database check on the Internet address, [redacted]. This Internet address (url) is registered to [redacted]

~~(+)~~
Am

[redacted] telephone number [redacted] e-mail address [redacted]

b7C

b7C

u
✓ i: [redacted]

See 1A(9)

288A-SF-133411-13

? JD.....DOB 3/1/85

- 1 -

FEDERAL BUREAU OF INVESTIGATION

Date of transcription 01/06/2003

SOURCE, who is not in a position to testify, was in contact with SA [redacted] via telephone and e-mail. SOURCE provided the following information:

b7C

[redacted]
[redacted] telephone number [redacted] is in control of several distributed denial of service (DDoS) networks. [redacted] lives with his mother, [redacted] has taken [redacted] computer away for getting in trouble with them previously, and has threatened to take them away permanently if he causes more trouble.

b7C

b3

[redacted] may be the owner of the Internet web site [redacted] and the file [redacted] is suppose to be a picture of [redacted] claims to run the Internet service business [redacted] also claims to be attacking every server on [redacted] IRC network simultaneously, Google (for one hour), and [redacted] last one for 12 hours). [redacted] also claims to have control of 85 compromised "gov" computers, including one "fbi" computer.

b7D

b7C

b3

[redacted]
[redacted] are installed on a compromised Internet computer, the attempt to connect to [redacted] The address resolved to different Internet protocol (IP) addresses at different times. On 01/06/03, the domain name resolved to all of the following IP addresses at the same time:

b7C

b2

b7C

b2

Investigation on 01/06/03 at Chicago

b2

File # 288A-SF-133411, 14

b7D

Date dictated 01/06/03by SA [redacted] MDA

b7C

288A-SF-133411-14

b2

b7D

288A-SF-113411, [redacted]

Continuation of FD-302 of SOURCE, On 01/06/03, Page 2

b7C

b2

[redacted]

On 01/08/03 at 9:00 [redacted] the domain name resolved to the IP address [redacted] and contained [redacted]

[redacted]

b7C

b7D

[redacted]

b2

[redacted]

[redacted] have conducted attacks on computers with the following Internet addresses:

IP address	date & time	type
[redacted]	01/05/03 23:32:52 GMT	packet
	01/05/03 23:34:45 GMT	packet
	01/05/03 23:30:32 GMT	packet
[redacted]	01/05/03 23:46:42 GMT	udp
	01/05/03 23:53:48 GMT	packet
	01/05/03 23:56:54 GMT	udp
[redacted]	01/05/03 23:57:12 GMT	udp
	01/05/03 23:45:38 GMT	packet
	01/05/03 23:56:04 GMT	packet
[redacted]	01/05/03 23:57:58 GMT	packet
	01/05/03 23:57:59 GMT	packet
	01/05/03 23:59:17 GMT	packet
[redacted]	01/06/03 00:01:37 GMT	packet
	01/03/03 15:50:25 GMT	packet
	01/03/03 16:02:30 GMT	packet
[redacted]	01/03/03 16:57:41 GMT	packet

b2

b7C

288A-SF-113411,

b2

b7D

Continuation of FD-302 of SOURCE, On 01/06/03, Page 3

01/03/03	17:51:45	GMT	packet
01/03/03	18:45:57	GMT	packet
01/03/03	18:53:28	GMT	packet
01/03/03	19:03:50	GMT	packet
01/03/03	19:09:23	GMT	packet
01/03/03	19:20:15	GMT	packet
01/03/03	19:41:25	GMT	packet
01/06/03	01:36:20	GMT	packet
01/06/03	01:40:17	GMT	packet
01/06/03	01:41:57	GMT	packet
01/06/03	01:44:04	GMT	packet
01/06/03	01:45:37	GMT	packet
01/06/03	01:46:09	GMT	packet
01/06/03	01:46:12	GMT	packet
01/06/03	01:46:13	GMT	packet
01/06/03	01:46:24	GMT	packet
01/06/03	01:46:44	GMT	packet
01/06/03	01:47:00	GMT	packet
01/06/03	01:47:12	GMT	packet
01/06/03	01:47:31	GMT	packet
01/06/03	01:47:39	GMT	packet
01/06/03	01:47:48	GMT	packet
01/06/03	01:48:19	GMT	packet
01/05/03	23:31:03	GMT	packet
01/05/03	23:35:11	GMT	packet
01/06/03	00:05:04	GMT	packet
01/03/03	18:43:58	GMT	packet
01/03/03	15:22:31	GMT	packet
01/03/03	18:31:59	GMT	packet
01/03/03	17:56:31	GMT	packet
01/03/03	17:56:39	GMT	packet
01/03/03	18:21:30	GMT	packet
01/03/03	18:24:16	GMT	icmp
01/03/03	18:24:25	GMT	icmp
01/03/03	17:53:42	GMT	packet
01/03/03	17:53:28	GMT	packet
01/03/03	15:41:36	GMT	packet
01/05/03	23:31:30	GMT	packet
01/03/03	18:26:19	GMT	packet
01/03/03	18:30:10	GMT	packet
01/03/03	18:30:10	GMT	packet
01/03/03	18:30:53	GMT	packet
01/03/03	18:31:06	GMT	packet
01/03/03	16:06:44	GMT	packet
01/03/03	16:07:23	GMT	packet

b7C

b2

288A-SF-113411, [REDACTED]

b2

b7D

Continuation of FD-302 of SOURCE, On 01/06/03, Page 4

[REDACTED]

01/03/03 17:55:35 GMT	packet
01/05/03 23:30:54 GMT	packet
01/05/03 23:35:35 GMT	packet

b7C

b2

[REDACTED] conducted attacks on computers with the following Internet addresses:

IP addressdate & timetype

b7C

[REDACTED]

01/06/03 02:49:11 GMT

udp

01/06/03 02:49:16 GMT

udp

b2

01/06/03 02:49:19 GMT

packet

[REDACTED]

01/06/03 02:11:02 GMT

packet

01/06/03 02:20:25 GMT

packet

[REDACTED] conducted the following attacks against the Google web site, www.google.com (IP address [REDACTED])

b7C

IP addressdate & timetype

b2

[REDACTED]

01/02/03 10:58:16 GMT

udp

01/02/03 10:58:23 GMT

packet

[REDACTED] also conducted the following attacks against the Google web site using the command [REDACTED] which caused [REDACTED]

b7C

b2

Webpagedate & time

http://www.google.com

01/02/03 10:58:54 GMT

http://www.google.com

01/02/03 10:58:54 GMT

http://www.google.com

01/02/03 10:58:54 GMT

http://www.google.com

01/02/03 10:58:55 GMT

http://www.google.com

01/02/03 10:58:55 GMT

[REDACTED] conducted attacks on computers with the following Internet addresses:

IP addressdate & timetype

b7C

[REDACTED]

01/06/03 19:21:45 GMT

packet

[REDACTED]

01/06/03 19:29:54 GMT

packet

b2

01/06/03 20:11:13 GMT

packet

[REDACTED] conducted attacks on computers with the following Internet addresses:

IP addressdate & timetype

b7C

[REDACTED]

01/06/03 21:33:55 GMT

packet

b2

- 1 -

FEDERAL BUREAU OF INVESTIGATION

Date of transcription 01/09/2003

SOURCE, who is not in a position to testify, was in contact with SA [redacted] via the telephone on 01/09/2003. SOURCE provided the following information: b7C

SOURCE identified [redacted]

[redacted] by his claimed ownership of [redacted] and by statements made by other hackers on IRC. b7C

Investigation on 01/09/2003 at Chicago, Illinois b2
File # 288A-SF-133411, [redacted] b7D dated 01/09/2003
by SA [redacted] *MAA* b7C

- 1 -

FEDERAL BUREAU OF INVESTIGATION

Date of transcription 01/14/2003

SOURCE, who is not in a position to testify, was in contact with SA [redacted] via telephone and email from 01/10/2003 to 01/13/2003. SOURCE provided the following information: b7C

[redacted] a distributed denial of service (DDoS) attack against Verio on 01/08/2003 with at least 1 Giga bit per second (Gbps) of data. Verio suffered a loss in reachability to various sites, and customers in Boca Raton, Florida suffered delays. b7C b3

[redacted] and a customer of Verio in Florida, suffered over \$5,000 in damages from the attack on 01/08/2003 against Verio and is willing to provide information to the FBI [redacted] [redacted] is located in [redacted] but can be reached at the following voice over Internet protocol (VOIP) telephone numbers located in the United States: [redacted] (main number), [redacted] (direct fax), [redacted] (direct phone). [redacted] can also be reach via the email address [redacted] Internet is a US-based company. b7C b7D

Investigation on 01/14/2003 at Chicago, Illinois b2
File # 288A-SF-133411, [redacted] b7D ctated 01/14/2003
by SA [redacted] MD4 b7C

SEE 141 (18)
288A-SF-133411-16

288A-SF-133411, [REDACTED]

b2

b7D

Continuation of FD-302 of SOURCE, On 01/14/2003, Page 2

b7C

b7D

[REDACTED]

The following information for [REDACTED] was obtained from the [REDACTED] on or about 01/11/2003:

b7C

Address: [REDACTED]

Email: [REDACTED]

b7D

The following information for [REDACTED] was obtained from the [REDACTED] on or about 01/11/2003:

b7C

Founder: [REDACTED]

Description: [REDACTED]

b7D

The following information for [REDACTED] was obtained from the [REDACTED] on or about 01/11/2003:

b7C

Founder: [REDACTED]

b7D

On or about 01/11/2003, [REDACTED] was listed as an operator for [REDACTED]. The following information for [REDACTED] was obtained from the [REDACTED] on or about 01/11/2003:

Address: [REDACTED]

URL: [REDACTED]

Email: [REDACTED]

b7C

b7D

The following information for [REDACTED] was obtained from the [REDACTED] on the [REDACTED] on or about 01/11/2003:

b7C

b7D

b2

b7D

288A-SF-133411,

A rectangular black box used for redaction, located to the right of the text '288A-SF-133411,'.

Continuation of FD-302 of SOURCE, On 01/14/2003, Page 3

A large rectangular black box used for redaction, spanning most of the width of the page below the header information.

b2

b7C

FEDERAL BUREAU OF INVESTIGATION

Precedence: ROUTINE

Date: 01/14/2003

To: San Francisco

Attn: Squad 14B/HRA

SA [REDACTED]

From: Chicago

Squad CY-2

Contact: SA [REDACTED]

b7C

Approved By: [REDACTED] *CDJ*

Drafted By: [REDACTED]

:mdh *MDH*

Case ID #: 288A-SF-133411-17 (Pending)

Title: UNSUB(S);
GOOGLE - VICTIM
SUNNYVALE, CA
NIPC - Impairment

Synopsis: To provide information on caption to San Francisco.

Enclosure(s): One (1) FD-302 from SOURCE information.
One (1) CD-R containing file [REDACTED]

b7C

Details: The previously listed FD-302 and CD-R are being provided to San Francisco on the captioned case.

288A SF-133411-17

To: San Francisco From: Chicago
Re: 288A-SF-133411, 01/14/2003

LEAD(s) :

Set Lead 1:

SAN FRANCISCO

AT HAYWARD, CALIFORNIA

Read and clear.

♦♦

FEDERAL BUREAU OF INVESTIGATION

Precedence: ROUTINE

Date: 01/09/2003

To: San Francisco

Attn: SA [REDACTED]

From: Chicago

Squad CY-2

Contact: SA [REDACTED]

b7C

Approved By: [REDACTED] *OC*

Drafted By: [REDACTED] *mdh*

Case ID #: 288A-SF-133411-18 (Pending)

Title: UNSUB(S)
GOOGLE - VICTIM
SUNNYDALE, CA
NIPC - Impairment

Synopsis: To provide source information to San Francisco.

Enclosure(s): One (1) FD-302 containing source information.

Details: The enclosed FD-302 contains source information relevant to the captioned case.

SEE 1A(12)

288A-SF-133411-18

To: San Francisco From: Chicago
Re: 288A-SF-133411, 01/09/2003

LEAD(s):

Set Lead 1:

SAN FRANCISCO

AT HAYWARD, CA

Read and clear.

♦♦

- 1 -

FEDERAL BUREAU OF INVESTIGATION

Date of transcription 01/08/2003

On Wednesday, January 8, 2003, SOURCE, who is in a position to testify, provided the following information to Special Agent (SA) [REDACTED] U.S. Department of Justice, Federal Bureau of Investigation (FBI), San Francisco Division:

b7C

[REDACTED]

b7D

[REDACTED] Boca Raton, Florida, telephone number [REDACTED] runs another [REDACTED] also runs the company [REDACTED] has been analyzing the attacks on [REDACTED] and may have additional information.

b7C

b7D

SOURCE does not have any additional information about [REDACTED]

b7C

The SOURCE e-mails are as follows:

Date: Sat, 04 Jan 2003 20:52:49 +0000
From: [REDACTED]
Reply-To: [REDACTED]
To: REDACTED
Subject: (Fwd) Update

b7C

b7D

This is a confidential update on the attacks. Expolits found the guy, and are going after him.

[REDACTED]

----- Forwarded message follows -----

Date sent: Sat, 04 Jan 2003 12:47:07 -0600 (CST)
From: [REDACTED]
Subject: Update
To: REDACTED

b7C

b7D

Investigation on 01/08/2003 at San Jose, California (telephonically)

File # [REDACTED] 288A-SF-133411 19 Date dictated _____

by SA [REDACTED] DM b7C

288A-SF-133411-19

[REDACTED]

b2

b7D

Continuation of FD-302 of Source, On 01/08/2003, Page 2

Copies to: **REDACTED**

Hi, team.

A status update is in order, and overdue. My apologies. Please keep all of this strictly between us. We don't want to ruin an on-going investigation.

[REDACTED]

b7D

Thoughts?

THANKS!

[REDACTED]

b7C

--
[REDACTED]

b7D

----- End of forwarded message -----
REDACTED

----- Forwarded message -----
Date: Sat, 04 Jan 2003 20:52:50 +0000
From: [REDACTED]
Reply-To: [REDACTED]
To: **REDACTED**

b7C

b7D

[Redacted]

b2

b7D

Continuation of FD-302 of Source, On 01/08/2003, Page 3

Subject: (Fwd) ADMIN: Update on the attacks

Another update.

[Redacted]

b7C

b7D

----- Forwarded message follows -----

Date sent: Sun, 05 Jan 2003 02:05:24 +1100

From: [Redacted]

Subject: ADMIN: Update on the attacks

b7C

To: REDACTED

b7D

Send reply to: [Redacted]

Hi Guys

[Redacted]

[Redacted]

b7D

[Redacted]

[REDACTED]

b2

b7D

Continuation of FD-302 of Source, On 01/08/2003, Page 4

[REDACTED]

[REDACTED]

b7D

I will keep you all posted as to our progress
and what action will be taken.

[REDACTED]

Regards

[REDACTED]

b7C

b7D

----- End of forwarded message -----

-REDACTED

Date: Wed, 8 Jan 2003 10:22:53 -0700 (MST)

b7C

From [REDACTED]

To: REDACTED

b7D

Subject: Request for limelight

[REDACTED]

[REDACTED]

b7D

[REDACTED] I'm not
sure that we need to call a vote for this so instead, I'm posting
here. If any of you feels that this really warrants a CFV, I'll
gladly call it.

thanks

b7D

[REDACTED]

FEDERAL BUREAU OF INVESTIGATION

Precedence: ROUTINE

Date: 01/08/2003

To: San Francisco

Attn: 14B/HRA

SA [redacted]

From: Chicago

Squad CY-2

Contact: SA [redacted]

Approved By: [redacted] *BCA*

Drafted By: [redacted]

:mdh *mdh*

b7C

Case ID #: 288A-SF-133411 *-20* (Pending)

Title: UNSUB(S);

Synopsis: To provide source and investigative information.

Enclosure(s): For SA [redacted] at San Francisco:

One (1) CD-R containing source email,
One (1) original and one (1) indexed copy of an FD-302
containing source information, and
One (1) original and one (1) indexed copy Insert
regarding U.S. Fish & Wildlife Service.

Details: The enclosed information is being provided to San Francisco for the cationed case.

SEE 7A(16)

288A SF-133411-20

To: San Francisco From: Chicago
Re: 288A-SF-133411, 01/08/2003

LEAD(s):

Set Lead 1:

SAN FRANCISCO

AT HAYWARD, CALIFORNIA

Read and clear.

♦♦

288A-SF-133411

MDH:mdh *mdh*

1

-21
An investigation was conducted on 01/06/2002 by SA [redacted] The following information was determined during the course of the investigation:

b7C

An Arin Whois lookup (www.arin.net) was conducted for the Internet address [redacted] (IP address [redacted]), a produced the following information:

b2

U.S. Fish and Wildlife Service IRM/BFO, HQ
755 Parfet St., Ste 349, Lakewood CO 80215

b2

SA [redacted] was in contact with [redacted] telephone number [redacted] and [redacted] telephone number [redacted] [redacted] who work for Incident Response for the U.S. Fish and Wildlife Service, regarding a computer intrusion on the previously identified computer. [redacted] stated that the Internet address is a dynamically assigned address that is part of a modem pool for dial up connections. [redacted] has had the compromised computer shipped to him in Colorado, and will provide whatever assistance he can to the FBI.

b7C

288A SF-133411-21

- 1 -

FEDERAL BUREAU OF INVESTIGATION

Date of transcription 01/28/2003

On January 13, 2003, SA [redacted] Federal Bureau of Investigation, San Francisco Division, Hayward Resident Agency, conducted the following investigation:

b7C

A record request was submitted to IOS [redacted] for [redacted] Records checks revealed [redacted] home address to be [redacted] This was changed from [redacted] due to a renumbering of addresses for a newly implemented emergency 911 system.

b7C

b3

[redacted] has been denied service with [redacted] because of illegal and improper activities.

b7C

b3

✓ "i: [redacted] .302"

b7C

Investigation on 1/13/2003 at Hayward, CaliforniaFile # 288A-SF-133411/22Date dictated Not Dictatedby SA [redacted] b7C

288A-SF-133411-22

Date 1-13-2003

☐ Birth ☐ Credit ☐ Criminal ☐ Death ☐ INS ☐ Marriage* ☐ Motor Vehicle ☒ Other see below

To <u>[redacted] b7C</u>	Buded
Return to <u>[redacted] b7C</u>	File number <u>288A-SF-133411</u>

Name and aliases of subject, applicant, or em <u>[redacted]</u>	b3
<u>[redacted]</u>	b7C

Addresses	<u>[redacted]</u>
Residence	
Business	
Former	

Limit to Lexis/Nexis + Choicepoint

*Date and place of marriage (if applicable) _____

Race	Sex <input type="checkbox"/> Male <input type="checkbox"/> Female	Age	Height	Weight	Hair	Eyes
Birth date	Birthplace					
Arrest Number	Fingerprint classification			Criminal specialty		
Social Security Number				Drivers License Number		

Specific information desired
Also verify address and owner of [redacted]

Results of check

ATTACHED

b7C

1-13-03
PM

US Postal Inspection Service Philadelphia Metro Division
Law Enforcement Agency Address Information Request Form

Request Received: Date/Time 1/15/2003 7:52 AM

Received by: FAX/McLean

Requesting Agency: F.B.I. San Francisco

Name

Telephone N

Fax Phone N

Information Requested

- ☐ Does Subject/Do Subjects Receive Mail at this Address? ☒ Forwarding Address(s) on File Subject(s) / Effective Date(s)
- ☐ Names of all / others who are receiving Mail at this Address ☐ All Forwarding Orders on file from this address
- ☐ Box Holder: All Information on Current Box Holder from PS Form 1093 on file with Post Office

Name(s)

Address

City:

Post Office or Agency to be Contacted

PO / Agen

Telephone No

2nd Telephone No

Fax No.:

Address Information Received
Please Use PS FORM 1093 Portion for PO BOX Info

b7C

☐ Mail is currently delivered for Subject(s) to above address.

All or Other Subject(s) for whom mail is delivered

Forwarding Orders/Effective Date on File for Subject(s)

Forwarding Orders/Effective Date on File for above address

Box Holder Information from PS FORM 1093

Box Holder _____ Date of Application _____

Applicant(s) _____ ID Provided / Number _____

Physical Address _____

Telephone # _____ Doing Business with the Public ☐ Yes ☐ No

All Persons / Entities currently receiving mail at Box _____

Request Completed by PPO _____ Date 1/15/03 0755h

Information given to Requestor by PPO _____

☐ Telephone ☒ Fax ☐ Voicemail ☐ Interoffice Mail ☐ Message left with _____

US Postal Inspection Service Philadelphia Metro Division
Law Enforcement Agency Address Information Request Form

Request Received: Date/Time 1/15/2003 7:52 AM

Received by: FAX/McLean

Requesting Agency: F.B.I. San Francisco

Name [REDACTED]

Telephone No [REDACTED]

Fax Phone No [REDACTED]

Information Requested

☐ Does Subject/Do Subjects Receive Mail at this Address?☒ Forwarding Address(s) on File Subject(s) / Effective Date(s)☐ Names of all / others who are receiving Mail at this Address☐ All Forwarding Orders on file from this address☐ Box Holder: All Information on Current Box Holder from PS Form 1093 on file with Post Office

Name(s) [REDACTED]

Address [REDACTED] *The new address due to 9/11*

b7C

City: [REDACTED]

Post Office or Agency to be Contacted

PO / Agency [REDACTED]

Telephone No [REDACTED]

2nd Telephone No [REDACTED]

Fax No.: [REDACTED]

Address Information Received

Please Use PS FORM 1093 Portion for PO BOX Info

☒ Mail is currently delivered for Subject(s) to above address. [REDACTED]All or Other Subject(s) for whom mail is delivered [REDACTED] *is the*Forwarding Orders/Effective Date on File for Subject(s) *name deleted**None on file*

Forwarding Orders/Effective Date on File for above address _____

Box Holder Information from PS FORM 1093

Box Holder _____

Date of Application _____

Applicant(s) _____

ID Provided / Number _____

Physical Address _____

Telephone # _____

Doing Business with the Public [] Yes [] No

All Persons / Entities currently re [REDACTED]

Form Completed by PPO [REDACTED]

Information given to Requestor by [REDACTED]

Date *1/15/03**0755/er*Date *1/15/03**0755/er*[] Telephone [] Fax [] Voicemail [] Interoffice Mail [] Message left with *FOS* [REDACTED]



b2

U.S. Department of Justice

Federal Bureau of Investigation

In Reply, Please Refer to
File No.

7142 Ambassador Road
Baltimore, MD 21244
April 3, 2000

[redacted]
[redacted] Police Department
[redacted] Avenue
[redacted] Delaware [redacted]

Dear Chief [redacted]

Enclosed is information concerning a complaint received
by the Federal Bureau of Investigation.

This information is being provided to your department
for whatever action deemed appropriate.

Sincerely yours,

Richard M. Mosquera
Special Agent in Charge

By: [redacted]

b7C

Supervisory Senior Resident Agent

258-BA-0-98
sh sh

Aut

esl0000001

6940000542

NOTE: Hand print names legibly; handwriting satisfactory for remainder.

Indices: ☒ Negative ☐ See below

Subject's name and aliases

Character of case

Computer Fraud Sq 14

Complaint received

☐ Personal ☒ Telephonic Date 3/29/2000 Time 2⁰⁰ pm

Comp

Complainant's DOB

Subject's Description	<input checked="" type="checkbox"/> Male	Height	Hair	Build	Birth date and birth place
	<input type="checkbox"/> Female	Weight	Eyes	Complexion	Social Security Number

Scars, marks and other data

Employer

Address

Telephone

Vehicle Description

Facts of complaint

The complainant, C, who wants to remain anonymous, is the subject, computer whic-kid

has been kicked out of several providers programs because of illegal improper activities. lives in the above address

SEARCHED	INDEXED
SERIALIZED	FILED
APR 07 2000	
FBI - BALTIMORE	

(Complaint received by)

BLOCK STAMP

b7C

Nebraska, Copyright 1998, All Rights Reserved.

End of search.

Use Browser Print Button to Print. You can return to the search results by clicking [here](#)

2. Click on the VIN search button at the bottom of the report.

Item	VIN	Year	Make	Registered Owner
------	-----	------	------	------------------

b7C

NO RECORDS FOR YOUR SUBJECT WERE FOUND IN THE FOLLOWING SECTION(S):

High Risk Addresses	N/A
DE Bankruptcies, Liens, and Judgm, Name & Address	N/A
NW Bankruptcies, Name & Social Security Number	N/A
DE Real Property Ownership	09/03/1991 through 07/17/2002
DE Property Owner by Subject's Address	09/03/1991 through 07/17/2002
Neighborhood Information	N/A
Demographic info. for most current address(es)	N/A
DE Uniform Commercial Code Filings	01/01/1996 through 11/30/2002
Watercraft by Name & State	00/00/0000 through 12/31/2001
FAA Aircraft Owners Search by Owner Name	00/00/0000 through 09/30/2002
FAA Airmen by Name	00/00/0000 through 08/31/2002

THE FOLLOWING DATABASES ARE NOT AVAILABLE:

DE Corporate Records by Name

Certain consumer information contained herein provided by InfoUSA, Omaha, Nebraska, Copyright 1998, All Rights Reserved.

End of search.

Use Browser Print Button to Print. You can return to the search results by clicking [here](#)

*****066138*****

SEND TO:

FBI-SF
450 GOLDEN GATE AVE FL 13
SAN FRANCISCO, CALIFORNIA 94102-3423

b7C

TAPE PRODUCED BY COUNTY: 5/1998

SUSSEX COUNTY, DE

Page 6

TAPE PRODUCED BY COUNTY: 7/2000

TAPE PRODUCED BY COUNTY: 7/1999

TAPE PRODUCED BY COUNTY: 7/2001

```
*****
*      13 PAGES      197 LINES      JOB  66138   116F5H      *
*      4:44 P.M. STARTED      4:44 P.M. ENDED      01/13/03      *
*****
*****
*      EEEEE      N      N      DDDD      *
*      E      N      N      D      D      *
*      E      NN      N      D      D      *
*      EEE      N      N      D      D      *
*      E      N      NN      D      D      *
*      E      N      N      D      D      *
*      EEEEE      N      N      DDDD      *
*****
*****
```

SEND TO:

FBI-SF
450 GOLDEN GATE AVE FL 13
SAN FRANCISCO, CALIFORNIA 94102-3423

b7C


Erase Your Online Tracks!
Automatically clean up your browser's cache, cookies, history, and much more!

My Computer:
☐ My cookie settings
☐ My browser cache
☐ My doc. history

Try it FREE!
Click here!

NETWORK-TOOLS.COM

NEW! Free Secondary DNS at Secondary.org!

Free Test - See if your e-mail server and client are vulnerable to viruses and worms

<input type="radio"/> Ping <input type="radio"/> Lookup <input type="radio"/> Trace <input type="radio"/> Xwhois	<input type="radio"/> DNS Records Click here for advanced NSlookup DNS tool <input type="radio"/> Network Lookup Whois Server: <input type="text" value="ARIN - Americas - whois.arin.net"/>	<input checked="" type="radio"/> Express Lookup <input type="radio"/> URL Unencode <input type="radio"/> URL Encode <input type="radio"/> HTTP Headers <input type="checkbox"/> SSL <input type="radio"/> E-mail Validation
---	--	--

☐ Convert Base-10 to IP

Submit

IP address
 No reverse lookup configured.
 Host name:

b7C

b2

TraceRoute to

Hop	(ms)	(ms)	(ms)	IP Address	Host name
1	0	0	0		
2	0	0	0		
3	0	0	16		
4	15	0	16		
5	31	15	32		
6	15	16	31		
7	16	31	31		
8	47	47	47		
9	47	46	47		
10	47	47	47		
11	47	47	62		
12	47	63	46		
13	47	62	63		

b7C

b2

Trace complete

Root: ICANN

Registration web site: Unknown

ICANN records: <http://www.iana.org/root-whois/tk.htm>

Notes: No known web site.

Updated: June 3, 2001

DNS Records for

query from dns.consumer.net to get an authoritative nameserver

NameServer used for query

Answer records

<input type="text"/>	1 MX	exchange:	<input type="text"/>	14400s
		server:	<input type="text"/>	
		email:	<input type="text"/>	
		serial:	<input type="text"/>	
		refresh:	<input type="text"/>	
		retry:	<input type="text"/>	
		expire:	<input type="text"/>	
<input type="text"/>	1 SOA	minimum ttl:	<input type="text"/>	
	1 NS	<input type="text"/>		
	1 NS	<input type="text"/>		
	1 A	<input type="text"/>		

b7C

b2

b7C

Authority records

Additional records

<input type="text"/>	1 A	<input type="text"/>
	1 A	<input type="text"/>

DNS Records for

query from dns.consumer.net to get an authoritative nameserver

NameServer used for query:

Answer records

<input type="text"/>	1 MX	exchange:	<input type="text"/>	0
		server:	<input type="text"/>	
		email:	<input type="text"/>	
		serial:	<input type="text"/>	
		refresh:	<input type="text"/>	

retry:

expire:

1 SOA minimum ttl:

1 NS

1 NS

1 A

Authority records

Additional records

1 A

1 A

Network IP address lookup:

whois whois.arin.net

b7C

b2

b2

OrgName: Network Operations Center Inc.

OrgID: NOC

NetRange:

CIDR:

NetName:

NetHandle:

Parent:

NetType:

NameServer:

NameServer:

Comment: ADDRESSES WITHIN THIS BLOCK ARE NON-PORTABLE

RegDate: 2002-05-31

Updated: 2002-05-31

b7C

b2

TechHandle:

TechName:

TechPhone:

TechEmail:

ARIN Whois database, last updated 2003-01-12 20:00

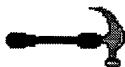
Enter ? for additional hints on searching ARIN's Whois database.

[Click Here for Tucows/GeoTrust SSL Certificates](#)

SPAMKILLER stops
SPAM before it hits
your in-box

[Anti-Virus.com](#)

SALE - Easy HangUp - \$12/\$20 for 2 - Free Shipping



Domain name not working? - See the Domain Troubleshooting Guide.

**Note: VeriSign (Network Solutions) is now blocking many whois queries.
To help reduce the load on their servers ... we have *reduced* the domain transfer/renewal fees
Transfer your domain away from Network Solutions now!
All time already paid to Network Solutions is carried over - No need to wait!**

**Domain Name Registration/Renewal with Tucows OpenSRS
com/net/org/info/biz/us domains now \$12.50/yr - See TheNic.com
Buy 5 or more years for just \$11.00 - 5 years for \$55
Buy 10 or more years for just \$10.75 - 10 years for \$107.50
No Hidden Charges, No Extra Fees!
Take full control of your domain records
Tucows is now the #2 registrar for .com/net/org domains**



-
- DNS server for Windows IIS. Great program when you need to manage numbers of DNS records and make frequent changes: Simple DNS Plus.
 - Hex gadget scripts used to create this web site are at <http://www.hexillion.com/software/>.

[redacted] b7C -

From:

To:

Sent: Wednesday, January 15, 2003 5:03 AM

Subject:

Due to Police/Fire emergency update in this community [redacted] is now

b7C

[redacted] There is no forwarding out of this residence. The name
delivered is [redacted]
Your Fax is being sent also.

b2

1/15/03

- 1 -

FEDERAL BUREAU OF INVESTIGATION

Date of transcription 01/28/2003

On January 21, 2003, SA [redacted] received a compact disk (CD) from [redacted] ~~NCC Security Response Team, Fish and Wildlife Services, work address 755 Parfet Street, Suite 349, Lakewood, Colorado, 80215.~~ The CD received contained data files from the machine [redacted] a computer on the network of the United States Department of Fish and Wildlife Services. The CD also contained a copy of a program known as the [redacted]

b7C

b2

(1)
An

b7C

✓ "i: [redacted] 01.302
02.Investigation on 1/21/2003 at Hayward, CaliforniaFile # 288A-SF-133411 / 23 Date dictated Not Dictated

by SA [redacted] b7C

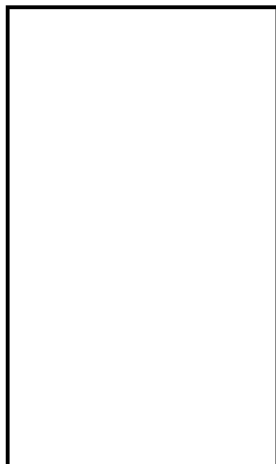
288A-SF-133411-23

- 1 -

FEDERAL BUREAU OF INVESTIGATION

Date of transcription 01/09/2003

On January 6, 2003, 1:30 P.M., SA [redacted] received an e-mail from SA [redacted] Federal Bureau of Investigation, Chicago Division. The email contained the following attachments: b7C

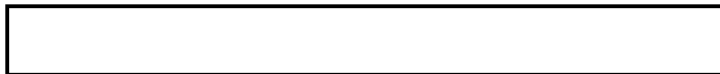
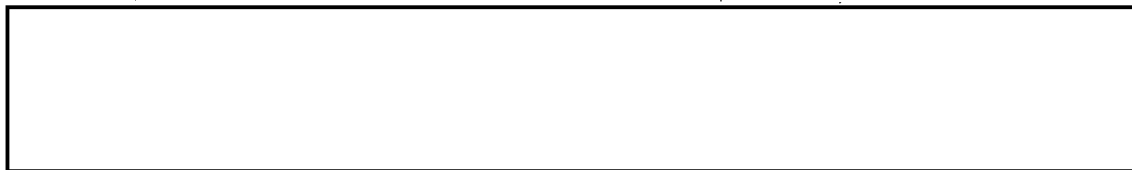


b7C

b2

Each attachment is listed below with its corresponding information:

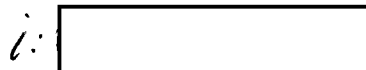
b7C



b2



u

302⁴

b7C

Investigation on 1/6/2003 at Hayward, CaliforniaFile # 288A-SF-133411 Date dictated Not Dictatedby SA [redacted] b7C

This document contains neither recommendations nor conclusions of the FBI. It is the property of the FBI and is loaned to your agency; it and its contents are not to be distributed outside your agency.

SEE 1A(10)

288A-SF-133411-24

288A-SF-133411

Continuation of FD-302 of _____, On 1/6/2003, Page 3

The authentication mechanism is simple. The user must be [redacted] and type:

[redacted]

b2

[redacted]

[redacted]

[redacted]

[redacted]

Here is his information:

b2

b7C

[redacted]

More attacks

All dates and times are GMT.

01/03 15:22:30 [redacted] packet
01/03 15:41:30 [redacted] packet
01/03 15:50:29 [redacted] packet
01/03 16:02:30 [redacted] packet
01/03 16:06:44 [redacted] packet
01/03 16:07:23 [redacted] packet

[redacted]

b7C

b2

b7C

[redacted]

This file is included in the associated FD-340.

288A-SF-133411

Continuation of FD-302 of _____

, On 1/6/2003

, Page 4

[redacted]

I've attached three logs from the [redacted] The botnet is run by [redacted] aka:

[redacted]

[redacted]

b2

b7C

[redacted]

He is assisted by [redacted] (who wrote the bot) and [redacted] is:

//name:

//b-day:

//location:

[redacted]

His web site is:

[redacted]

[redacted] has put out a call for additional ircd resources:

[redacted]

The botnet is on [redacted] This resolves to different IPs at different times (moving the bots), and is presently [redacted] This IP is in the Sprint network and is registered to:

b7C

[redacted]

b7C

The channel is [redacted] and it has no key. The bots are controlled by a simple authentication mechanism; an oper types [redacted] (no

[redacted]

b2

b7C

288A-SF-133411

Continuation of FD-302 of

, On 1/6/2003

, Page

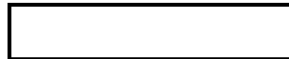
5



b2

They claim to have 12K bots; I suspect the number is somewhat higher now. I have logged 10018 unique IPs in the [redacted] the list of IPs and hostnames is attached below.

If you need any other data, please let me know.



This file is included in the associated FD-340.

b7C



b2

01/03 15:22:31 packet
01/03 15:41:36 packet
01/03 15:50:25 packet
01/03 16:02:30 packet
01/03 16:06:44 packet
01/03 16:07:23 packet
01/03 16:57:41 packet
01/03 17:51:45 packet
01/03 17:53:28 packet
01/03 17:53:28 packet
01/03 17:53:42 packet
01/03 17:55:35 packet
01/03 17:55:49 packet
01/03 17:55:49 packet
01/03 17:56:31 packet
01/03 17:56:39 packet
01/03 18:21:30 packet
01/03 18:24:16 cmp 1
01/03 18:24:25 cmp 1
01/03 18:26:19 packet
01/03 18:30:10 packet
01/03 18:30:10 packet
01/03 18:30:47 packet
01/03 18:30:53 packet
01/03 18:31:03 packet
01/03 18:31:06 packet
01/03 18:31:20 packet
01/03 18:31:52 packet
01/03 18:31:59 packet
01/03 18:43:58 packet

b7C

288A-SF-133411

Continuation of FD-302 of _____, On 1/6/2003, Page 6

01/03 18:45:57 [redacted] packet [redacted]
01/03 18:53:28 [redacted] packet [redacted]
01/03 19:03:50 [redacted] packet [redacted]
01/03 19:09:23 [redacted] packet [redacted]
01/03 19:20:15 [redacted] packet [redacted]
01/03 19:41:25 [redacted] packet [redacted]

b7C

b2

[redacted] A .gov host has been infected and joined the [redacted]
[redacted] Here are the details, with all dates and times GMT:

b7C

01/03 20:14:29 [redacted]

joined [redacted]

[redacted] It is unclear if this
host actually launched any attacks.

[redacted]

[redacted] may be the owner of the web site, [redacted] His supposed
picture, from the web site, is attached to this note as [redacted]

b7C

[redacted]

I have included below a log of [redacted] chatting with another miscreant. In
it he admits to attacking www.google.com as well as

[redacted] He also admits to owning .gov boxes, including
a fbi.gov host. His bot estimates are a bit inflated, but I do believe
he has at least [redacted]

b7C

, On 1/6/2003

, Page 13

[illegible]

b7C

b2

[illegible]

This file is included in the associated FD-340.

b7C

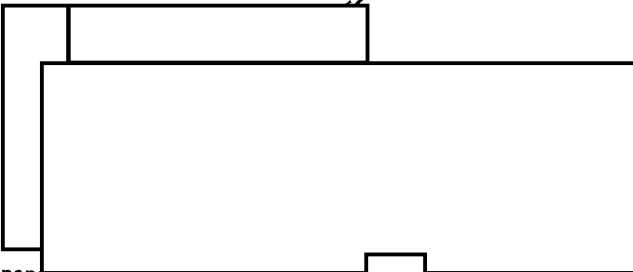
Here are the logs from the attack against www.google.com

All dates and times are GMT.

288A-SF-133411

Continuation of FD-302 of _____, On 1/6/2003, Page 14

01/02 10:58:16
01/02 10:58:23
01/02 10:58:54
01/02 10:58:54
01/02 10:58:54
01/02 10:58:55
01/02 10:58:55



b7C
b2

Here the bots respond to the packeting attack issued by _____ and times are GMT.

01/02 11:05:39 _____ packeting _____ with 32mb traffic

This file is included in the associated FD-340.

- 1 -

FEDERAL BUREAU OF INVESTIGATION

Date of transcription 01/08/2003

b7C
b7D [redacted] an employee of GOOGLE.COM, cell phone number [redacted] work phone number [redacted] was interviewed on January 7, 2003. After being advised of the identity of the Agent and the nature of the interview, [redacted] provided the following information:

[redacted] received an address range of Internet Protocol (IP) Addresses, used in the January 2, 2003, Denial of Service (DOS) attack on GOOGLE.COM, from [redacted]. Upon researching, one IP was found to have connected to GOOGLE.COM three times during the attack day. This IP links back to [redacted]

During the morning DOS attack on GOOGLE.COM, January 2, 2003, the spike of incoming traffic received by GOOGLE.COM occurs at the same time as commands executed on [redacted] Internet Relay Chat (IRC) Channel. The morning attack indicated that each attacking computer was performing [redacted] commands. The DOS attack in the afternoon was the same as the DOS attack in the morning. (21) *Am*

GOOGLE.COM has made hardware changes to their servers to prevent similar future attacks. This includes the ability to save [redacted]

b2

Investigation on 1/7/2003 at Hayward, California (telephonically)

File # 288A-SF-133411 Date dictated Not Dictated

by SA [redacted]

b7C

02,302 b7C*See 1A(11)**288A-SF-133411-25*

FEDERAL BUREAU OF INVESTIGATION

Precedence: ROUTINE

Date: 01/17/2003

To: San Francisco

From: San Francisco

14B/HRA

Contact: SA [REDACTED]

Approved By: [REDACTED]

b7C

Drafted By: [REDACTED]

:am

Case ID #: 288A-SF-133411 (Pending)

Title: CHANGED

[REDACTED]
GOOGLE - VICTIM
SUNNYVALE, CA
NIPC - Impairment

b7C

b3

Synopsis: To change the title to reflect the subject identification.

b7C

Previous Title: Title marked "Changed" to reflect UNSUB(S) being identified as [REDACTED] Title previously carried as "UNSUB(S);GOOGLE - VICTIM; SUNNYVALE, CA; NIPC - Impairment".

b3

Details: Investigation has led to the identification of [REDACTED] as the subject [REDACTED] is responsible for several computer intrusions and Denial of Service (DOS) attacks [REDACTED] commits the DOS attacks by [REDACTED]

b7C

b2

b7C

6:1 [REDACTED] 01. EC"

*Poster
Pls change
Title
Thank
me
1-17-03*

288A-SF-133411-26

FEDERAL BUREAU OF INVESTIGATION

Precedence: ROUTINE

Date: 01/31/2003

To: Chicago

From: San Francisco
14B/HRA

Contact: SA [REDACTED]

Approved By: [REDACTED]

b7C

Drafted By: [REDACTED]:am

Case ID #: 288A-SF-133411 - 27 (Pending)

Title: [REDACTED]

b7C

GOOGLE - VICTIM
SUNNYVALE, CA
NIPC - Impairment

b3

Synopsis: To set lead to Chicago to provide source information as necessary.

Details: Google.com was a victim of two Denial of Service (DOS) attacks on January 2, 2003. The first attack occurred around 4:00 A.M. PST, lasting approximately five to seven minutes, and affected Google.com's Santa Clara servers. The second attack occurred around 3:00 P.M. PST, lasting approximately five to seven minutes, and affected both Google.com's Santa Clara and Virginia servers. The first attack was a DOS attack comprised of both UDP and Ping Flood attacks. The second attack was on a much larger scale and consisted of a SYN Flood attack.

Investigation has led to the identification of [REDACTED] as the subject [REDACTED] is responsible for several computer intrusions and Denial of Service (DOS) attacks [REDACTED] commits the DOS attacks by [REDACTED]

b7C

b2

San Francisco Division requests Chicago Division interview appropriate sources and report positive information.

b7C

EC

288A-SF-133411-27

To: Chicago From: San Francisco
Re: 288A-SF-133411, 01/31/2003

LEAD(s):

Set Lead 1:

CHICAGO

AT CHICAGO, IL

Please provide source information, as necessary, on activity regarding; the Internet Relay Chat (IRC) nic [redacted] the IRC channel [redacted] and the domain names [redacted] and [redacted]. Please collect pertinent log files and other electronic evidence and interviews and forward to writer.

b7C

♦♦

- 1 -

FEDERAL BUREAU OF INVESTIGATION

Date of transcription 01/31/2003

On January 31, 2003, SA [] received an e-mail from [] NCC Security Response Team, Fish and Wildlife Services, work telephone number [] The email is attached to and part of this document. b7C

(1.2.3.4)
Am

Investigation on 1/31/2003 at Hayward, CaliforniaFile # 288A-SF-133411-28 Date dictated Not Dictated

by SA []

[att.com home](#)[AT&T Business](#)[HOME](#) | [HELP CENTER](#) | [> ACCOUNT CENTER](#) | [ABOUT US](#)[MANAGE E-MAIL](#)[MANAGE USER ID](#)[WEB MAIL](#)[Check Mail](#)[New Message](#)[Address Book](#)[Distribution Lists](#)

View Message

From: [redacted]@fws.gov

[SAVE SENDER](#)To: nccs-sf@fbi.gov

cc: [redacted]@fws.gov

Date: Fri, January 31, 2003 08:38:00

Subject: Attention [redacted]

[VIEW HEADER](#)[VIEW BODY](#)[LOG OFF](#)

[redacted]

I've attached the setup.bat file and ir.conf file as you requested for FBI Case#288a-sf-13341. The ir.conf file has the IRC configuration ie., channel and userid. I hope this helps. Let me know if you need anything else.

[redacted]

NCC Security Response Team

	setup.bat
	ir.conf

[FORWARD MAIL](#) [REPLY](#) [REPLY TO ALL](#) [DELETE](#)[NEXT MESSAGE](#) [RETURN](#) [HELP](#)[LEGAL](#) | [PRIVACY](#) | [SERVICE TERMS](#) | [CONTACT US](#)

Copyright © 2002, AT&T All Rights Reserved.

[att.com home](#)

[AT&T Business](#)



AT&T Business
Internet Services

[HOME](#) | [HELP CENTER](#) | [ACCOUNT CENTER](#) | [ABOUT US](#)

[MANAGE E-MAIL](#)

[MANAGE USER ID](#)

[WEB MAIL](#)

[Check Mail](#)

[New Message](#)

[Address Book](#)

[Distribution Lists](#)

View Message

From  fws.gov

[SAVE SENDER](#)

To: nccs-sf@fbi.gov

cc :

Date: Fri, January 31, 2003, 10:37:00

Subject: re:Attentio 

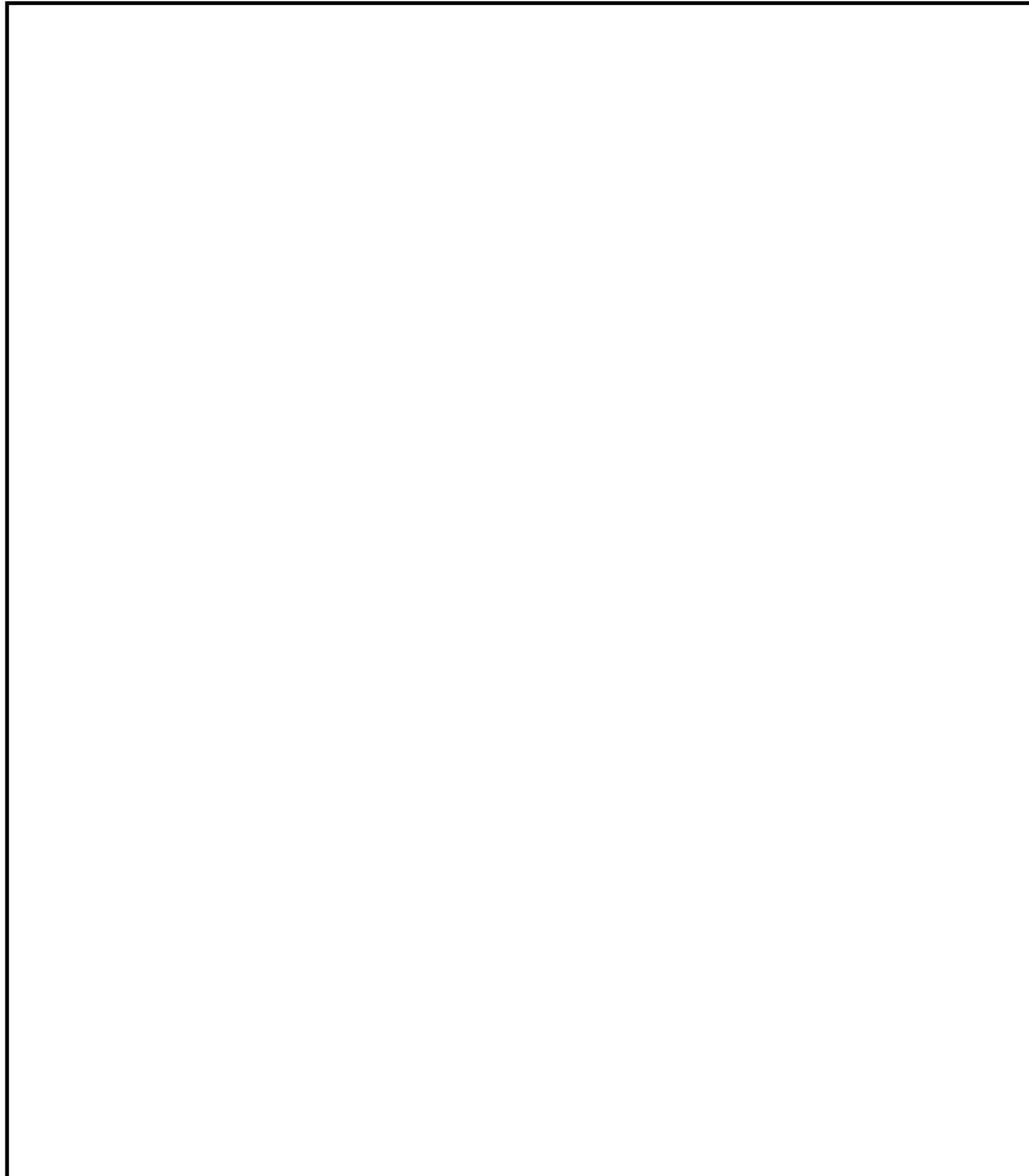
[VIEW HEADER](#)

[VIEW BODY](#)

b2

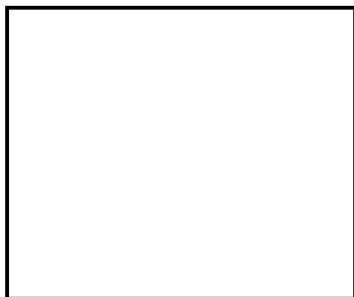
b7C

[LOG OFF](#)



:noerrors

:end



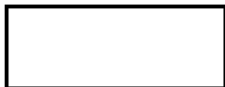
b7C

NCC Security Response Team

nccs-sf@fbi.gov

01/31/2003 10:32 AM

To: [redacted] gov,
cc: [redacted] ws.gov,
Subject: re:Attention [redacted]



I couldn't view or open the .bat file. Can you send the contents plain text so I can view and save them? Thanks again for your help.

b7C

b7C

SA [redacted]
Federal Bureau of Investigation

[\[X\] FORWARD MAIL](#) [\[X\] REPLY](#) [\[X\] REPLY TO ALL](#) [\[X\] DELETE](#)
[\[X\] NEXT MESSAGE](#) [\[X\] RETURN](#) [\[X\] HELP](#)

[LEGAL](#) | [PRIVACY](#) | [SERVICE TERMS](#) | [CONTACT US](#)

Copyright © 2002, AT&T All Rights Reserved.

- 1 -

FEDERAL BUREAU OF INVESTIGATION

Date of transcription 01/23/2003

On January 23, 2003, SA [redacted] Federal Bureau of Investigation, San Francisco Division, Hayward Resident Agency, conducted the following investigation:

b7C

A Network Internet Protocol (IP) Address Lookup was performed on the following Domain Name and associated IP Address:

Domain Name [redacted]

IP Address: [redacted]

b7C

b2

The address [redacted] was associated with [redacted] telephone number [redacted] as the managing organization, as well as technical contact.

Investigation on 1/23/2003 at Hayward, CaliforniaFile # 288A-SF-133411Date dictated Not Dictated

by SA [redacted]

b7C

This document contains neither recommendations nor conclusions of the FBI. It is the property of the FBI and is loaned to your agency; it and its contents are not to be distributed outside your agency.

288A-SF-133411-29

- 1 -

FEDERAL BUREAU OF INVESTIGATION

Date of transcription 01/23/2003

On January 23, 2003, SA [redacted] Federal Bureau of Investigation, San Francisco Division, Hayward Resident Agency, conducted the following investigation: b7C

A Network Internet Protocol (IP) Address Lookup was performed on the following Domain Name and associated IP Address:

Domain Name: [redacted]

IP Address: [redacted] b7C b2

The address was associated with [redacted]

[redacted] telephone number [redacted]
[redacted] fax number [redacted] is the managing organization,
as well as technical contact.

b7C

Investigation on 1/23/2003 at Hayward, CaliforniaFile # 288A-SF-133411Date dictated Not Dictated

by SA [redacted]

b7C

This document contains neither recommendations nor conclusions of the FBI. It is the property of the FBI and is loaned to your agency; it and its contents are not to be distributed outside your agency.

288A-SF-133411-30

- 1 -

FEDERAL BUREAU OF INVESTIGATION

Date of transcription 01/23/2003

On January 23, 2003, SA [redacted] Federal Bureau of Investigation, San Francisco Division, Hayward Resident Agency, conducted the following investigation:

b7C

A Network Internet Protocol (IP) Address Lookup was performed on the following Domain Name and associated IP Address:

Domain Name: [redacted]

b7C

b2

IP Address: [redacted]

The address [redacted] is associated with [redacted] as the managing organization, as well as technical contact.

Investigation on 1/23/2003 at Hayward, California

File # 288A-SF-133411-31 Date dictated Not Dictated

by SA [redacted]

b7C

This document contains neither recommendations nor conclusions of the FBI. It is the property of the FBI and is loaned to your agency; it and its contents are not to be distributed outside your agency.

288A-SF-133411-31

288A-SF-133411 -32
AM:am

1

b7C

On January 23, 2003, SA [redacted] Federal Bureau of Investigation, San Francisco Division, Hayward Resident Agency, conducted the following investigation:

A Network Internet Protocol (IP) Address Lookup was performed on the following Address:

IP Address:

[redacted]

b2

b7C

The address was associated with

[redacted]

[redacted]

✓ call [redacted] INS

b7C

288A-SF-133411-32

STOP TELEMARETERS

NETWORK=TOOLS.COM

Featured Product - GFI LANguard Network Security Scanner

Scans your entire network, IP by IP, for possible security holes. Free for non commercial use

<input type="radio"/> Ping <input type="radio"/> Lookup <input type="radio"/> Trace <input type="radio"/> Xwhois	<input type="radio"/> DNS Records Click here for advanced NSLookup DNS tool NEW Free Secondary DNS at Secondary.org!	<input checked="" type="radio"/> Express Lookup <input type="radio"/> URL Unencode <input type="radio"/> URL Encode <input type="radio"/> HTTP Headers <input type="checkbox"/> SSL <input type="radio"/> E-mail Validation
	<input type="radio"/> Network Lookup Whois Server: <input type="text"/>	

b7C

☐ Convert Base-10 to IP

IP address:

Host name:

Alias:

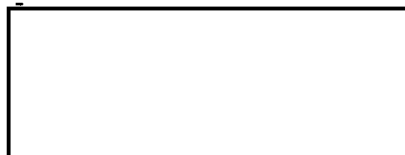
b2

TraceRoute to

b7C

Hop	(ms)	(ms)	(ms)	IP Address	Host name
1	0	0	0	<input type="text"/>	<input type="text"/>
2	0	0	0		
3	16	15	0		
4	16	0	15		
5	16	31	15		
6	16	15	16		
7	Timed out	Timed out	Timed out		
8	16	31	31		
9	Timed out	Timed out	Timed out		
10	125	125	63		
11	78	63	62		
12	94	78	78		

13	62	78	63
14	63	203	78
15	62	78	79
16	250	250	250
17	Timed out	Timed out	Timed out
18	Timed out	Timed out	Timed out
19	Timed out	Timed out	Timed out
20	Timed out	Timed out	Timed out



b7C

Trace aborted.

Third Level Domains are Registered under .au.

You are attempting to look up a level 2 domain.

WHOIS whois.aunic.net net.au:

% Copyright 2001 auDA. Terms of Use at <http://www.aunic.net/copyright.html>

The object shown below is NOT in the AUNIC database.
 It has been obtained by querying a remote server:
 (whois.ausregistry.net.au) at port 43.
 To see the object stored in the AUNIC database
 use the -R flag in your query.

Domain net.au has been reserved by auDA

%%% End of referred query result

.au is for Australia

Root: ICANN

Registration web site: <http://www.aunic.net/>

Whois server: whois.aunic.net

Whois web interface: <http://www.nic.at/>

Third Level Domains Registered

Cost: AU\$55, US\$27 for .com.au. Most other domains are free.

ICANN records: <http://www.iana.org/root-whois/au.htm>

Notes: com.au, net.au, org.au, edu.au, and gov.au, id.au, asn.au, info.au, oz.au, telememo.au, csiro.au, conf.au, otc.au (to be removed) are registered. au has a series of unclear restrictions including place names and generic words see <http://www.inwww.com/policies/comaupolicy.php3>

Updated: May 3, 2001

.au

is not in the Xwhois database

DNS Records for net.au:

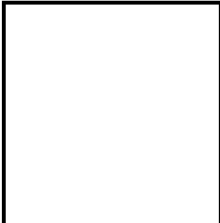
query from dns.consumer.net to get an authoritative nameserver

NameServer used for query: **ns1.ausregistry.net**

Answer records

	server:	ns1.ausregistry.net	
	email:	dns@ausregistry.net.au	
	serial:	2002093056	
	refresh:	14400	
	retry:	5400	
	expire:	2678400	
net.au	1 SOA	minimum ttl:	86400 86400s
net.au	1 NS	audns01.syd.optus.net	86400s
net.au	1 NS	ns1.ausregistry.net	86400s
net.au	1 NS	ns2.ausregistry.net	86400s
net.au	1 NS	ns3.ausregistry.net	86400s
net.au	1 NS	ns3.melbourneit.com	86400s
net.au	1 NS	ns4.ausregistry.net	86400s
net.au	1 NS	dns1.telstra.net	86400s
net.au	1 NS	au2ld.csiro.au	86400s

Authority records**Additional records**

ns1.ausregistry.net	1 A		3600s
ns2.ausregistry.net	1 A		3600s
ns3.ausregistry.net	1 A		3600s
ns4.ausregistry.net	1 A		3600s
au2ld.csiro.au	1 A		4624s
audns01.syd.optus.net	1 A		14179s

b7C

DNS Records for tmns.net.au

query from dns.consumer.net to get an authoritative nameserver

NameServer used for query: **sy-dns01.tmns.net.au**

Answer records

tmns.net.au	1 NS	sy-dns01.tmns.net.au	86400s
tmns.net.au	1 NS	sy-dns02.tmns.net.au	86400s
	server:	sy-dns01.tmns.net.au	
	email:	dvm@onaustralia.com.au	
	serial:	2002062601	
	refresh:	3600	

	retry:	1800
	expire:	2592000
tmns.net.au	1 SOA minimum ttl:	86400 86400s
	preference:	10
tmns.net.au	1 MX exchange:	extmail.bigpond.com 86400s

Authority records



Additional records


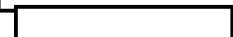



sy-dns01.tmns.net.au	1 A		86400s
sy-dns02.tmns.net.au	1 A		86400s
extmail.bigpond.com	1 A		7200s
extmail.bigpond.com	1 A		7200s

b7C

Network IP address lookup:





whois whois.arin.net 

OrgName: 
OrgID: 

NetRange: 
CIDR: 
NetName: 
NetHandle: 
Parent: 

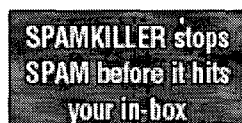
b7C

NetType: Direct Assignment
NameServer: SY-DNS01.TMNS.NET.AU
NameServer: SY-DNS02.TMNS.NET.AU
Comment:
RegDate: 1996-01-22
Updated: 2002-08-09

TechHandle: 
TechName: 
TechPhone: 
TechEmail: 

ARIN Whois database, last updated 2003-01-30 20:00
Enter ? for additional hints on searching ARIN's Whois database.

[Click Here for Tucows/GeoTrust SSL Certificates](#)



[Anti-Virus.com](#)

SALE - Easy HangUp - \$12/\$20 for 2 - Free Shipping



Domain name not working? - See the Domain Troubleshooting Guide.

**Note: VeriSign (Network Solutions) is now blocking many whois queries.
To help reduce the load on their servers ... we have *reduced* the domain transfer/renewal fees
Transfer your domain away from Network Solutions now!
All time already paid to Network Solutions is carried over - No need to wait!**

**Domain Name Registration/Renewal with Tucows OpenSRS
com/net/org/info/biz/us domains now \$12.50/yr - See TheNic.com**

Buy 5 or more years for just \$11.00 - 5 years for \$55

Buy 10 or more years for just \$10.75 - 10 years for \$107.50

No Hidden Charges, No Extra Fees!

Take full control of your domain records

Tucows is now the #2 registrar for .com/net/org domains



-
- **DNS server for Windows IIS. Great program when you need to manage numbers of DNS records and make frequent changes: Simple DNS Plus.**
 - **Hex gadget scripts used to create this web site are at <http://www.hexillion.com/software/>.**

- 1 -

FEDERAL BUREAU OF INVESTIGATION

b3 Rule 6(e)

Date of transcription 02/03/2003

b7C

GRAND JURY MATERIAL - DISSEMINATE PURSUANT TO RULE 6(e)

Pursuant to a United States District Court, Northern
District of California, Federal Grand Jury Subpoena dated [redacted]
[redacted] provided the following
information:

[redacted]

Return service from the Subpoena is attached to and a
part of this document.

(1)
Am

Investigation on 2/3/2003 at Hayward, California (via facsimile)File # 288A-SF-133411 Date dictated Not Dictatedby SA [redacted]

b7C

fax message

date: January 31, 2003

b3

to: Special Agent [redacted]
Federal Bureau of Investigation**fax:** [redacted]

b2

b7C

from: [redacted]**pages:** 5 (including cover sheet)

b7C

☐ Urgent☐ For Review☐ Please Comment☐ Please Reply**COMMENTS:**

- 1 -

FEDERAL BUREAU OF INVESTIGATION

Date of transcription 02/03/2003b3 Rule 6(e)
b7C**GRAND JURY MATERIAL - DISSEMINATE PURSUANT TO RULE 6(e)**

Pursuant to a United States District Court, Northern
District of California, Federal Grand Jury Subpoena dated [redacted]
[redacted] provided the
following information:

[redacted]

Return service from the Subpoena is attached to and a
part of this document.

①
Am

i: [redacted] 01.302

Investigation on 2/3/2003 at Hayward, California (via facsimile)File # 288A-SF-133411 Date dictated Not Dictated

b7C

by SA [redacted]

288A-SF-133411-34

- 1 -

FEDERAL BUREAU OF INVESTIGATION

Date of transcription 02/04/2003

On February 4, 2003, SA [redacted] received an e-mail from [redacted] cell phone number [redacted]. The e-mail follows:

b7C

From: [redacted]

To: nccs-sf@fbi.gov

cc :

Date: Tue, February 04, 2003, 13:35:00

Subject: Fw: Threatened attack on a root-server and my IRC server

----- Original Message -----

From: [redacted]

To:

Sent: Tuesday, February 04, 2003 12:54 PM

Subject: Threatened attack on a root-server and my IRC server

b7C

> -----BEGIN PGP SIGNED MESSAGE-----

> [redacted]

>

> Greetings. [redacted] sent your address my way, after I asked him for

> any contacts he has due to the claim of an attack on a root-server.

>

> I can be reached at [redacted] (cell) anytime if you want to talk in

> person.

>

> Background:

>

> A user known as [redacted] which I understand has already attracted the

> FBI's attention) has flooded various IRC network servers and users off

> the face of the planet. Using compromised computer systems (most

> running windows, thanks microsoft) he's able to cause a sustained 800

> megabit to multiple gigabit floods of any host in a very small bit of

> time.

b7C

✓ i: [redacted] 01.302

Investigation on 2/4/2003 at Hayward, CaliforniaFile # 288A-SF-133411 - 35Date dictated Not Dictatedby SA [redacted] b7C

288A-SF-133411-35

PTT/MP
UPLOADED
5cc.
2-7-0

288A-SF-133411

Continuation of FD-302 of _____

, On 2/4/2003 , Page 2

>
> Another user, known as [REDACTED] has a similar capability, although it
> may be quite a bit smaller. He can still hit and maintain 500
> megabits/sec without much problem.
>
> I believe they know each other, and work together.
>
> I have several logs of discussions with [REDACTED] in which he claims
> he does not attack [REDACTED] but does use his [REDACTED]
> for other goals, like [REDACTED]
>
> At one point, someone mentioned to [REDACTED] that attacking
> [REDACTED] (my machine) would be stupid, since it would also
> attack a DNS root server. Today, I got this in my mailbox:
>
> Date: 4 Feb 2003 [REDACTED]
> Message-ID: [REDACTED]
> To: [REDACTED]
> Subject: He [REDACTED] Webmail]
> [REDACTED]
> From: [REDACTED]
>
> Hope you enjoy [REDACTED]
> [REDACTED] it will be mad fun knowing
> I'm owning a root-server too. ;D
>
> This is from a web comment form, where people can enter their return
> address. I therefore doubt following up on the "from" address will be
> of use.
>
> The IP address that contacted our web server to send this message is
> [REDACTED] which is a HTTP proxy maintained by [REDACTED]. They
> have no logs (they disabled it because of the huge amount of data it
> generated) but have turned on logging now. I can provide you with the
> contact there and the email we've exchanged if that helps.
>
> I believe this threat is very real, and they will begin in the next 72
> hours [REDACTED] has threatened other networks [REDACTED] and one other)
> and [REDACTED] is likely to [REDACTED] which is why
> [REDACTED]
>
> I believe [REDACTED] email address is [REDACTED]
> although I don't know if that's a real address or a fake one, or if he
> or a friend controls that domain.
>

b7C

b7D

b7C

b7C

288A-SF-133411

Continuation of FD-302 of _____, On 2/4/2003, Page 3

> -
> -----BEGIN PGP SIGNATURE-----
> Version: GnuPG v1.2.1 (NetBSD)
> Comment: See http:// for my keys

b7C

>
>
> -----END PGP SIGNATURE-----
>

b7C

FEDERAL BUREAU OF INVESTIGATION

Precedence: DEADLINE 02/14/2003

Date: 02/07/2003

To: Baltimore

From: San Francisco
14B/Hayward
Contact: [REDACTED]

Approved By: [REDACTED]

b7C

Drafted By: [REDACTED]

am

Case ID #: 288A-SF-133411 - 36 (Pending)

Title: [REDACTED]

b7C

GOOGLE - VICTIM
SUNYVALE, CA
NIPC - Impairment
01/02/2003

b3

12
Am

Synopsis: To set lead to Baltimore to provide descriptive data of residence.

Details: Google.com was a victim of two Denial of Service (DOS) attacks on January 2, 2003. The first attack occurred around 4:00 A.M. PST, lasting approximately five to seven minutes, and affected Google.com's Santa Clara servers. The second attack occurred around 3:00 P.M. PST, lasting approximately five to seven minutes, and affected both Google.com's Santa Clara and Virginia servers. The first attack was a DOS attack comprised of both UDP and Ping Flood attacks. The second attack was on a much larger scale and consisted of a SYN Flood attack.

Investigation has led to the identification of [REDACTED] as the subject. [REDACTED] is responsible for several computer intrusions and Denial of Service (DOS) attacks. [REDACTED] commits the DOS attacks by [REDACTED]

b2

San Francisco Division requests Baltimore Division provide descriptive data for the residence to be searched.

b7C

b3

✓ i: [REDACTED] BALTIMORE EC

b7C

288A-SF-133411-36

To: Baltimore From: San Francisco
Re: 288A-SF-133411, 02/07/2003


LEAD(s) :

Set Lead 1:

BALTIMORE

AT SEAFORD, DELAWARE

Please provide descriptive data of building; to include exterior color, roof composition and color, building number and location of building number, exact street location and orientation, location and orientation of access points to the building, location and description of fences or other buildings on the property, and photographs (if possible) of the building at



b7C

♦♦



- 1 -

FEDERAL BUREAU OF INVESTIGATION

Date of transcription 02/13/2003

On February 13 2003 11:18:00 A.M., SA [redacted]
received an e-mail from [redacted] Vice President and General Counsel for GOOGLE, work telephone number [redacted] e-mail address [redacted] A summary of the e-mail follows: b7C

[redacted] estimates the damages from a January 2, 2003, Denial of Service attack to be approximately \$49,500. These damages are inclusive of the lost revenue associated with the downtime incurred, liability cost to GOOGLE's Search Partners, and direct labor cost of GOOGLE employees. b7C

i: [redacted] 302
Investigation on 2/13/2003 at Hayward, California

File # 288A-SF-133411-37 Date dictated Not Dictated

by SA [redacted]

- 1 -

FEDERAL BUREAU OF INVESTIGATION

Date of transcription 02/07/2003**GRAND JURY MATERIAL - DISSEMINATE PURSUANT TO RULE 6(e)**

b3 Rule 6(e)

b7C

Pursuant to a United States District Court, Northern
District of California, Federal Grand Jury Subpoena dated [REDACTED]
[REDACTED] provided the
following information:

[REDACTED]

Return service from the Subpoena is attached to and a
part of this document.

①
\$m

Investigation on 2/7/2003 at Hayward, California (via facsimile)File # 288A-SF-133411 Date dictated Not Dictatedby SA [REDACTED]

b7C

STATEMENT OF CONFIDENTIALITY

THE INFORMATION CONTAINED IN THIS FAX IS INTENDED FOR THE EXCLUSIVE USE OF THE ADDRESSEE AND MAY CONTAIN CONFIDENTIAL OR PRIVILEGED INFORMATION. IF YOU ARE NOT THE INTENDED RECIPIENT, YOU ARE HEREBY NOTIFIED THAT ANY FORM OF DISSEMINATION OF THIS COMMUNICATION IS STRICTLY PROHIBITED. IF THIS FAX WAS SENT TO YOU IN ERROR, PLEASE IMMEDIATELY NOTIFY US BY PHONE.

Total Number of Pages, including Cover: 9

b3 Rule 6 (e), FGJ

Name: SA

b7C

Location: FBI - San Francisco CAFAX #: Date: 2 / 6 / 2003From: Re:

Enclosed please find the records which, consistent with the Electronic Communications Privacy Act, 18 U.S.C. §2703 (c)(1)(C)(as amended), respond to your request on _____, your file # _____.

If this matter results in an arrest or prosecution, please contact us if you need any additional information. If you have any questions regarding our response, please contact me at

- 1 -

FEDERAL BUREAU OF INVESTIGATION

Date of transcription 02/19/2003

SOURCE, who is not in a position to testify, was in contact with SA [redacted] via email on 02/03/2003. SOURCE provided the following information:

b7C

The domain name server (DNS) zone file for [redacted] contains the following entries:

[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]

b2

b7C

Investigation on 02/19/2003 at Chicago, IllinoisFile # 288A-SF-133411, 42 Date dictated 02/19/2003by SA [redacted] MJA

b2

b7C

b7D

This document contains neither recommendations nor conclusions of the FBI. It is the property of the FBI and is loaned to your agency; it and its contents are not to be distributed outside your agency.

288A-SF-133411-42

- 1 -

FEDERAL BUREAU OF INVESTIGATION

Date of transcription 02/20/2003

SOURCE, who is not in a position to testify, was in contact with SA [redacted] from 01/02/2003 to 02/20/2003. SOURCE provided the following information:

b7C

The Internet relay chat (IRC) server [redacted] channel [redacted] hosts a distributed denial of service (DDoS) network. Several individuals have committed numerous DDoS attacks from [redacted]

The attacks used include the [redacted] attacks. Attacks on Internet web sites are also committed by [redacted]

b7C

[redacted]. The DDoS network [redacted] was also used to scan for and infect additional host Internet computers with the BOT using the [redacted] command.

b2

SOURCE provided log files of [redacted] which contained, in part, the following information:

01/02 10:52:55
01/02 10:52:55
01/02 10:52:56
01/02 10:55:23
01/02 10:55:25
01/02 10:55:30
01/02 10:55:39
01/02 10:58:16
01/02 10:58:23
01/02 10:58:54
01/02 10:58:54
01/02 10:58:54
01/02 10:58:54
01/02 10:58:55
01/02 10:58:55
01/02 10:58:55
01/02 10:58:55
01/02 10:58:55
01/02 11:02:12
01/02 11:04:10
01/02 11:04:17

b7C

b2

Investigation on 02/20/2003 at Chicago, Illinois

File # 288A-SF-133411, 43

Date dictated 02/20/2003

b2

by SA [redacted] MDH

b7C

b7D

288A-SF-133411-43

FEDERAL BUREAU OF INVESTIGATION

Precedence: ROUTINE

Date: 02/25/2003

To: Baltimore

Attn: SA [REDACTED]

From: San Francisco

14B/Hayward

Contact: SA [REDACTED]

b7C

Approved By: [REDACTED]

Drafted By: [REDACTED]

Case ID #: 288A-SF-133411 - (Pending)

Title: [REDACTED]

GOOGLE - VICTIM
SUNNYVALE, CA
NIPC - Impairment
01/02/2003

b7C

b3

Synopsis: To set lead to Baltimore to request assistance in executing a search warrant.

Administrative: SA [REDACTED] contacted SA [REDACTED] on February 25, 2003, and discussed the scope and depth of the search and interview to be performed at [REDACTED] Delaware.

b7C

Enclosure(s): Search affidavit and associated attachment A and attachment B are provided in hard copy and soft copy format. FD-302's referenced on search affidavit hard copy are also provided.

Details: Google.com was a victim of two Denial of Service (DOS) attacks on January 2, 2003. The first attack occurred around 4:00 A.M. PST, lasting approximately five to seven minutes, and affected Google.com's Santa Clara servers. The second attack occurred around 3:00 P.M. PST, lasting approximately five to seven minutes, and affected both Google.com's Santa Clara and Virginia servers. The first attack was a DOS attack comprised of both UDP and Ping Flood attacks. The second attack was on a much larger scale and consisted of a SYN Flood attack.

Investigation has led to the identification of [REDACTED] as the subject. [REDACTED] is responsible for several computer intrusions and Denial of Service (DOS) attacks. [REDACTED] commits the DOS attacks by [REDACTED]

b7C

b3

b2

(

SEARCH.EC

b7C

288A-SF-133411-44

To: Baltimore From: San Francisco
Re: 288A-SF-133411, 02/25/2003

[REDACTED]

b2

The property to be searched is [REDACTED]

[REDACTED] Delaware. This is a residential home occupied by [REDACTED]

[REDACTED] Social Security
Number [REDACTED], born [REDACTED] Delaware Drivers
License [REDACTED] No other individuals are known to reside at

b7C

[REDACTED] owns a 1992 Buick Century
Custom Station Wagon automobile, Vehicle Identification Number
[REDACTED]

b3

Details of the search and interview were discussed
between SA [REDACTED] and SA [REDACTED] on February 25, 2003. SA [REDACTED]
has enclosed all requested information and documentation.

b7C

San Francisco Division requests the assistance of
Baltimore Division, Dover Resident Agency, in executing a search
warrant.

To: Baltimore From: San Francisco
Re: 288A-SF-133411, 02/25/2003

LEAD(s) :

Set Lead 1:

BALTIMORE

AT [REDACTED] DELAWARE

Please provide assistance in executing a search warrant. Documentation, including the search affidavit, associated attachments, and supporting FD-302's are enclosed.

b3

Upon execution of the search warrant at [REDACTED]
[REDACTED] Delaware, please interview [REDACTED]
if present. Questions of particular interest are as follows:

b7C

b2

b7C

Please provide [REDACTED] the contact information for Special Agent [REDACTED] San Francisco Division, Hayward Resident Agency. Inform [REDACTED] that [REDACTED] will be in contact with him regarding evidence seized and further interviewing.

b7C

b3

♦♦

FEDERAL BUREAU OF INVESTIGATION

Precedence: ROUTINE

Date: 02/19/2003

To: San Francisco

Attn: Squad 14B/HRA

SA [REDACTED]

From: Chicago

Squad CY-2

Contact: SA [REDACTED]

Approved By: [REDACTED] *CB*

b7C

Drafted By: [REDACTED]

mdh MDA

Case ID #: 288A-SF-133411

(Pending) ✓ - 45

Title: UNSUB(S);
GOOGLE - VICTIM
SUNNYVALE, CA
NIPC - Impairment

Synopsis: To provided information to San Francisco on captioned case.

Enclosure(s): For SA [REDACTED]

b7C

One (1) original FD-302, and
One (1) indexed copy of FD-302.

Details: Information regarding the zone file for the domain name server [REDACTED] is provided on the enclosed FD-302.

b7C

050mdh 05.ec 288A-SF-133411-45

To: San Francisco From: Chicago
Re: 288A-SF-133411, 02/19/2003

LEAD(s):

Set Lead 1:

SAN FRANCISCO

AT HAYWARD, CA

Read and clear.

♦♦

FEDERAL BUREAU OF INVESTIGATION

Precedence: ROUTINE

Date: 02/21/2003

To: San Francisco

Attn: SA [REDACTED]

From: Chicago

Squad CY-2

Contact: SA [REDACTED]

b7C

Approved By: [REDACTED] *LP*

Drafted By: [REDACTED]

mdh mdt

Case ID #: 288A-SF-133411

(Pending) ✓ - 46

Title: [REDACTED]

GOOGLE - VICTIM

SUNNYVALE, CA

NIPC - Impairment

b7C

b3

Synopsis: To provide information on the captioned case to San Francisco.

Enclosure(s): To SA [REDACTED]

b7C

One (1) original and one (1) indexed copy of FD-302, and

One (1) FD-340 containing one (1) CDR with IRC log of [REDACTED]
channel [REDACTED]

b7C

Details: The enclosed information is being provided to San Francisco for the captioned case.

SEE 1A(20)

052mdh01.ec

288A-SF-133411-46

To: San Francisco From: Chicago
Re: 288A-SF-133411, 02/21/2003

LEAD(s):

Set Lead 1:

SAN FRANCISCO

AT HAYWARD, CA

Read and clear.

♦♦

288A-SF-133411 - 47
AM:am

1

On March 5, 2003, 10:30 A.M. PST, Special Agent (SA) [redacted] Federal Bureau of Investigation, San Francisco Division, Hayward Resident Agency, received a phone call from [redacted] work telephone number [redacted] is with the Delaware State Police Department.

b7C

[redacted] and SA [redacted] discussed the details of [redacted] investigation of [redacted] is responsible for [redacted]

Am

b7C

b3

[redacted] offered assistance in executing a warrant on the home of [redacted] is writing a search warrant, to encompass financial documents and computer media, for the residence of [redacted] requests copies of computer media, if seized, for review on his case.

b7C

b3

✓ 6.1 [redacted] INS

b7C

288A-SF-133411-47

- 1 -

FEDERAL BUREAU OF INVESTIGATION

Date of transcription 01/17/2003

Source, who is not in a position to testify, provided the following information:

Two companies were effected by a recent Distributed Denial of Service (DDOS) attack initiated [redacted] web hosting company was victim to a DOS attack on their server. Initial estimates indicate that the attack cost the company approximately \$2,000. A second company, [redacted] suffered a DDOS concurrently. [redacted] is an e-business solutions company [redacted] loses to date are approximately \$5,000. Both companies purchase bandwidth from [redacted] which is a United States based company. Network traffic for both companies goes through [redacted] servers in northern Virginia. The attacks occurred on 01/09/03 and the victims or hosts are infected with the [redacted]

b2
b7C

He/she provided the following log of [redacted] chat:

1,2
SR

b2
b7C

b2

Investigation on 01/17/2003 at Falls Church, Virginia

File # [redacted] 288A-SF-133411 48 Date dictated _____

by [redacted]

This document contains neither recommendations nor conclusions of the FBI. It is the property of the FBI and is loaned to your agency; it and its contents are not to be distributed outside your agency.

SR010603.302

288A-SF-133411-48

[redacted] 288A-SF-133411

b2

b7D

Continuation of FD-302 of

[redacted]

, On 01/17/2003, Page 2

[redacted]

The user [redacted] is actually

[redacted]

b2

b7C

b3

[redacted]

FEDERAL BUREAU OF INVESTIGATION

Precedence: ROUTINE

Date: 03/26/2003

To: San Francisco

Attn: SSA [redacted]

From: San Francisco

Squad 14B, Hayward RA

Contact: SA [redacted]

b7C

Approved By: [redacted] *[Signature]*

Drafted By: [redacted] *[Signature]*

Case ID #: 288A-SF-133411 (Pending)
288-SF-C128668 (Pending) *49*

Title: [redacted]

GOOGLE-VICTIM
SUNNYVALE, CA
NIPC-IMPAIRMENT

b7C

b3

Synopsis: NIPCIP/Computer Intrusion Squad IIIA accomplishments

Details: The purpose of this EC is to claim IIIA statistics for the San Francisco Division's NIPCIP/Computer Intrusion Squad.

b7C

I: [redacted] 085RMP01.FD542

288A-SF-133411-49

To: San Francisco From: San Francisco
Re: 288A-SF-133411, 03/26/2003

Accomplishment Information:

Number: 1
Type: NIPCIP VICTIM CONTACTED/INTERVIEWED
ITU: AGENT INTERVIEW
ITU: NIPCIP
Claimed By:
SSN:
Name:
Squad: 14B

Number: 1
Type: NIPCIP SUBJECT TOOL/EXPLOIT/MALICIOUS CODE IDENTIFIED
ITU: COMPUTER ASSISTANCE
ITU: NIPCIP
Claimed By:
SSN:
Name:
Squad: 14B

b7C

Number: 1
Type: NIPCIP SUBJECT IDENTIFIED
ITU: COMPUTER ASSISTANCE
ITU: NIPCIP
Claimed By:
SSN:
Name:
Squad: 14B

♦♦

FEDERAL BUREAU OF INVESTIGATION

Precedence: ROUTINE

Date: 04/01/2003

To: San Francisco

Attn: SA [REDACTED]

From: San Francisco

14B/HRA

Contact: SA [REDACTED]

b7C

Approved By: [REDACTED]

Drafted By: [REDACTED]

am

b2

b7D

Case ID #: 288A-SF-133411 (Pending) -52

288A-SF-129533 (Pending)

[REDACTED] (Pending)

Title: [REDACTED]

b7C

b3

GOOGLE-VICTIM;
SUNNYVALE, CA;
NIPC-IMPAIRMENT

Synopsis: To request access to the Internet Proxy for Internet investigations.

Details: Google.com was a victim of two Denial of Service (DOS) attacks on January 2, 2003, affecting Google.com's Santa Clara and Virginia servers. The first attack was a DOS attack comprised of both UDP and Ping Flood attacks. The second attack was on a much larger scale and consisted of a DOS SYN Flood attack.

Investigation has led to the identification of [REDACTED]
[REDACTED] as the subject [REDACTED] is responsible
for several computer intrusions and Denial of Service (DOS)
attacks [REDACTED] commits the DOS attacks by [REDACTED]

b2

b7C

b3

San Francisco Division requests the assistance of San Francisco Division, San Jose Resident Agency, in providing access to the Internet proxy to further investigations.

b7C

*Router
Set reach 4/8/03
SA [REDACTED]
4/3/03
288A-SF-133411-V2*

To: San Francisco From: San Francisco
Re: 196E-SF-133512, 04/01/2003

LEAD(s):

Set Lead 1: (Action)

SAN FRANCISCO

AT SAN JOSE, CA

Please create a user account with the name "GOOGLE".
This account will be used for the afore mentioned cases when
conducting Internet investigations.

♦♦

- 1 -

FEDERAL BUREAU OF INVESTIGATION

Date of transcription 04/16/2003

b7C [redacted] a Detective with the Delaware State Police Department. work telephone number [redacted] contacted Special Agent (SA) [redacted]. After being advised of the identity of the Agent and the nature of the interview, [redacted] provided the following information:

b7C [redacted] contacted SA [redacted] regarding the details of a State of Delaware, County of Sussex, search warrant, executed on the residence of [redacted]
[redacted]

b3 [redacted] owns two computers, one running a MICROSOFT WINDOWS-XP Operating System (OS) and the other running a REDHAT LINUX OS. [redacted] also possesses two digital cameras, a Personal Data Assistant (PDA), and numerous compact disks (CD) with various content. [redacted] also has memory devices, for use in the PDA and cameras, as well as a memory device reader attached to one of the computers.

[redacted] interviewed [redacted] during the search. During the interview, [redacted] provided the following information:

[Large redacted area]

i: [redacted] 13341156.302

Investigation on 4/16/2003 at Hayward, California (telephonically)

File # 288A-SF-133411 Date dictated Not Dictated

by SA [redacted]

288A-SF-133411-√3

288A-SF-133411

b7C

Continuation of FD-302 of

[Redacted]

, On 4/16/2003

, Page 2

[Redacted]

b3

b7C

A copy of the items seized from the search, [Redacted]
notes during the interview, and a photograph of [Redacted] are stored
in the 1A portion of this case file.



U.S. Department of Justice

United States Attorney
Northern District of California

280 S. First Street, Suite 371
San Jose, California 95113

FAb2

March 27, 2003

VIA U.S. MAIL

Federal Bureau of Investigation
22320 Foothill Blvd., #530
Hayward, CA 94541

ATTN: S/A

b7C

Re:

b2

U.S. v. Unsub (google.com) - File No. 2003R00115

As you are aware, materials received by the grand jury pursuant to subpoena will be disclosed to you pursuant to Rule 6(e)(3)(A) of the Federal Rules of Criminal Procedure, which provides in pertinent part:

Disclosure otherwise prohibited by this rule of matters occurring before the grand jury other than to its deliberations and the vote of any grand juror, may be made to --

(ii) such government personnel . . . as are deemed necessary by an attorney for the government to assist an attorney for the government in the performance of such attorney's duty to enforce criminal law.

In connection with the disclosure of this information, however, please be advised that Rule 6(e)(3)(B) provides:

Any person to whom material is disclosed under subparagraph (A)(ii) of this paragraph shall not utilize that grand jury material for any purpose other than assisting the attorney for the government in the performance of such attorney's duty to enforce federal criminal law. An attorney for the government shall promptly provide the district court, before which was empaneled the grand jury whose material has been so disclosed, with the names of the persons to whom such disclosure has been made.

Pursuant to the above quoted requirement, your name has been supplied to the district court as an individual to whom disclosure has been made.

288A-SF-133411-54

If other agents are assigned to the cases referenced above, please provide this office with the names of those persons to whom disclosure will be made prior to such disclosure, so their names may be reported to the court as well.

If you have any questions, please do not hesitate to call me at (408

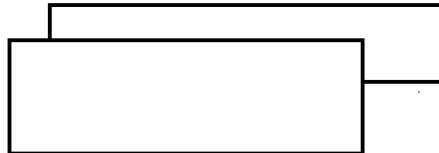


b2

Very truly yours,

KEVIN V. RYAN
United States Attorney

ADAM BRAUN
United States Attorney



b7C

Legal Assistant

AB:jy



U.S. Department of Justice

Federal Bureau of Investigation

In Reply, Please Refer to
File No. 288A-SF-133411

450 Golden Gate Ave.
PO Box 36015
San Francisco, CA 94102
(415) 553-7400
April 18, 2003

Kevin V. Ryan
United States Attorney

United States Attorney's Office
450 Golden Gate Avenue, 11th Floor
San Francisco, CA 94102

Attention: AUSA Adam Braun

Dear Mr. Braun:

This letter is in response to our April 14, 2003, conversation regarding deferring Federal prosecution, in the above captioned case, to the State of Delaware, County of Sussex, District Attorney's Office.

Google.com was a victim of two Denial of Service (DOS) attacks on January 2, 2003, affecting Google.com's Santa Clara and Virginia servers. The first attack was a DOS attack comprised of both UDP and Ping Flood attacks. The second attack was on a much larger scale and consisted of a DOS SYN Flood attack. Damages, provided from Google.com, estimate the damages to be approximately \$50,000.

Investigation has led to the identification of [redacted]
[redacted] as the subject [redacted]

[redacted] is responsible for several
computer intrusions and Denial of Service (DOS) attacks.
[redacted] commits the DOS attacks by [redacted]

[redacted] has intruded into both private and
protected computers.

A State of Delaware, County of Sussex, search warrant was lawfully executed on April 15, 2003. In conjunction with the search warrant, [redacted] was arrested by and taken into the custody of the State of Delaware Police Department. The search warrant yielded several computers and computer peripherals seized. A Federal search warrant is currently being sought for review of the items lawfully seized.

b7C

b3

b2

b7C

b3

b7C

1: [redacted] DEFER. LTR

288A-SF-133411 - JT

On April 14, 2003, during a conversation with Special Agent [REDACTED] AUSA Braun deferred prosecution to the local authorities, the State of Delaware, County of Sussex, District Attorney's Office.

b7C

Please contact SA [REDACTED] with any questions.

Sincerely,

Mark J. Mershon
Special Agent in Charge

By:

b7C

[REDACTED]
Supervisory Special Agent

FEDERAL BUREAU OF INVESTIGATION

✓ Precedence: ROUTINE

Date: 04/21/2003

To: San Francisco

Attn: SA [redacted]
Hayward RA

From: Baltimore

17/Dover RA

Contact: SA [redacted]

Approved By: [redacted] MB/ [signature]

b7C

Drafted By: [redacted]

Case ID #: 288A-SF-133411-56 (Pending)

b7C

Title: [redacted]

b3

GOOGLE - Victim
Sunnyvale, CA on 1/02/03
NIPC - Impairment
OO : SF

Synopsis: Investigation at [redacted] DE on 4/15/03. Arrest.
interview of captioned subject [redacted]

b7C

b3

Reference: 288A-SF-133411 Serial 44

Package Copy: Being forwarded under separate cover: Delaware.
State Police search warrant, arrest warrant, and investigative
reports re [redacted]

Enclosure(s): The original and one copy of the FD-302, dated
4/15/03, interview of [redacted] 1-A with original
notes of the [redacted] interview.

Details: On Tuesday, 4/15/03, captioned subject [redacted]
[redacted] was arrested without incident at his residence [redacted]
[redacted] A search warrant was executed at the
residence concurrent with the arrest. Both the search warrant
and the arrest warrant were issued by the Superior Court of the
State of Delaware. FBI Baltimore, Dover RA, assisted in the
arrest and interview of [redacted]

b7C

b3

288A-SF-133411-56

To: San Francisco From: Baltimore
Re: 288A-SF-133411, 04/21/2003

Evidence obtained from the search, including a "mirror image" of the subject's computer hard drive, will be forwarded to FBI San Francisco by the DSP.

This lead is covered.

To: San Francisco From: Baltimore
Re: 288A-SF-133411, 04/21/2003

LEAD(s) :

Set Lead 1: (Info)

SAN FRANCISCO

AT HAYWARD RA

Read and clear.

♦♦

- 1 -

FEDERAL BUREAU OF INVESTIGATION

Date of transcription 04/23/2003

[redacted] a Detective with the Delaware State Police b7C
Department, work telephone number [redacted] contacted Special
Agent (SA) [redacted] provided the following
information:

b7C

b3

[redacted] arrested on April 15, 2003 b7C
[redacted] mother, has informed
[redacted] that she will not pay the bond to release [redacted]

[redacted] received several UNITED PARCEL SERVICE
(UPS) packages, at her residence, for [redacted] is
bringing the UPS packages to [redacted] for investigation.

[redacted] will try and re-interview [redacted] in the next few
days. The prior interview, on April 15, 2003, was recorded on audio
tape and was incomplete due to a faulty audio recorder.

b7C

b3

b7C

i: [redacted] 133411SG.302

Investigation on 4/22/2003 at Hayward, California (telephonically)File # 288A-SF-133411 Date dictated Not Dictated

by SA [redacted]

b7C

SEE 100231

288A-SF-133411-18

Memorandum



To : SAC SAN FRANCISCO

Date 04/29/03

From : SA [REDACTED]

b7C

Subject : [REDACTED]

b2

b7D

Dates of Contact		
04/28/03		
File #s on which contacted (Use Titles if File #s not available)		
288A-SF-133411		
Purpose and results of contact		
<input type="checkbox"/> NEGATIVE <input type="checkbox"/> POSITIVE (See attached) <input checked="" type="checkbox"/> STATISTIC 7c.		
Description of Statistical Accomplishment	Title of Case	File No.
7c. INFORMATION USED IN SEARCH WARRANT	UNSUB(S); GOOGLE - VICTIM SUNNYVALE, CA NIPC - IMPAIRMENT 01/02/2003	288A-SF-133411
* SEE ATTACHED COPY OF S/W EXECUTED BY THE STATE OF DELAWARE, COUNTY OF SUSSEX, PAGE 10 OF AFFIDAVIT, PARAGRAPH 20.		
Information herein obtained confidentially; informant's name is not to be disclosed in a report or otherwise unless it has been definitely decided that this person is to be a witness in a trial or hearing.		
PERSONAL DATA		

1

1

1

Init

(5)

AND

1- SA

1- SA

b7C

see reverse side for statistics

288A-SF-133411-61

STATISTICAL ACCOMPLISHMENTS
Criminal Informant/Cooperative Witness (CI/CW)

1. Number of Subjects Arrested:

- a. FBI
- b. Other Federal Agencies
- c. State and Local Agencies

2. Number of Subjects/Victims Identified and/or Located:

- a. FBI
- b. Other Federal Agencies
- c. State and Local Agencies

3. Number of Investigative Matters Initiated:

- a. FBI
- b. Other Federal Agencies
- c. State and Local Agencies

4. Number of Disseminations Based Upon CI/CW Information:

5. Number of Violent Acts Prevented:

6. Number of Times CI/CW Information Used in Title III Affidavits:

- a. FBI
- b. Other Federal Agencies
- c. State and Local Agencies

7. Number of Times CI/CW Information Used in Search Warrant Affidavits:

- a. FBI
- b. Other Federal Agencies
- c. State and Local Agencies

8. Number of Times CI/CW Information Used in Obtaining Complaint/Information/Indictment:

- a. FBI
- b. Other Federal Agencies
- c. State and Local Agencies

9. Merchandise Recovered (Value):

- a. FBI
- b. Other Federal Agencies
- c. State and Local Agencies

10. Asset/Property Seized (Value at Time of Seizure):

- a. FBI
- b. Other Federal Agencies
- c. State and Local Agencies

11. Monetary Value of Asset/Property Actually Forfeited to Government:

\$ _____

12. Number of Convictions Obtained as a Result of Information Furnished by CI/CW or as a Result of other Significant Operational Assistance Furnished:

- a. FBI
- b. Other Federal Agencies
- c. State and Local Agencies

13. Number of Times Undercover Agent or Other Law Enforcement Officer Introduced into an Investigative Matter by CI/CW:

- a. FBI
- b. Other Federal Agencies
- c. State and Local Agencies

14. Drugs Recovered (Wholesale Value):

- a. FBI
- b. Other Federal Agencies
- c. State and Local Agencies

15. Number of Consensually Monitored Conversations CI/CW participated in:

- a. FBI
- b. Other Federal Agencies
- c. State and Local Agencies

☒ Additional information may be added by attaching another form or a plain sheet of paper for additional entries.
☐ See codes on reverse side.
☒ Requires that an explanation be attached and loaded into SRAA for recovery over \$1m and PELP over \$5m.

For Further Instructions See: MAOP, Part I, Sections 3-5 thru 3-5.3.

PROPERTY CODES

01 Cash
02 Stocks, Bonds or Negot. Instruments
03 General Retail Merchandise
04 Vehicles
05 Heavy Machinery & Equipment
06 Aircraft
07 Jewelry
08 Vessels
09 Art, Antiques or Rare Collections
11 Real Property
20 All Other

SENTENCE TYPES

CP Capital Punishment
JS Jail Sentence
LP Life Parole
LS Life Sentence
NS No Sentence (Subject is a Fugitive,
Insane, has Died, or is a
Corporation)
PB Probation
SJ Suspension of Jail Sentence
YC Youth Correction Act

PELP CODES

22 Counterfeit
Stocks/Bonds/Currency/
Negotiable Instruments
23 Counterfeit/Pirated Sound
Recordings or Motion Pictures
24 Bank Theft Scheme Aborted
25 Ransom, Extortion or Bribe
Demand Aborted
26 Theft From or Fraud Against
Government Scheme Aborted
27 Commercial or Industrial
Theft Scheme Aborted
30 All Other

RACE CODES

A Asian/Pacific Islander
B Black
I Indian/American
U Unknown
W White
X Nonindividual

AGENCY CODES

AFOIS Air Force Office of Special Investigations
ACIS Army Criminal Investigative Service
BATF Bureau of Alcohol, Tobacco & Firearms
BLA Bureau of Indian Affairs
DCAA Defense Contract Audit Agency
DCIS Defense Criminal Investigative Service
DEA Drug Enforcement Administration
DOC Department of Corrections
DOI Dept. of Interior
EPA Environmental Protection Agency
FAA Federal Aviation Administration
FDA Food and Drug Administration
HHS Dept. of Health & Human Services
HUD Dept. of Housing & Urban Development
INS Immigration and Naturalization Service
IRS Internal Revenue Service
NASA Nat'l Aeronautics & Space Admin
NBIS Nat'l NARC Border Interdiction
NCIS Naval Criminal Investigative Service
RCMP Royal Canadian Mounted Police
SBA Small Business Administration
USBP U.S. Border Patrol
USCG U.S. Coast Guard
USCS U.S. Customs Service
USDS U.S. Department of State
USMS U.S. Marshals Service
USPS U.S. Postal Service
USSS U.S. Secret Service
USTR U.S. Treasury
LOC Local
CITY City
COUN County
ST State
OTHR Other

JUDGMENT CODES

CJ Consent Judgment
CO Court Ordered Settlement
DF Default Judgment
DI Dismissal
JN Judgment Notwithstanding
MV Mixed Verdict
SJ Summary Judgment
VD Verdict for Defendant
VP Verdict for Plaintiff

JUDICIAL OUTCOME

AG Agreement
BR Barred/Removed
CC Civil Contempt
DC Disciplinary Charges
FI Fine
PI Preliminary Injunction
PR Temporary Restraining Order
PS Pre-filing Settlement
RN Restitution
SP Suspension
VR Voluntary Resignation
OT Other

SUBJECT PRIORITY

A Subject wanted for crimes of violence
(i.e., murder, manslaughter, forcible
rape) against another individual or
convicted of such a crime in the past five
years
B Subject wanted for crimes involving loss
or destruction of property valued in
excess of \$25,000 or convicted of such a
crime in the past five years.
C All other subjects.

SUBJECT DESCRIPTION CODES

ORGANIZED CRIME
SUBJECTS

1F Boss
1G Underboss
1H Consigliere
1J Acting Boss
1K Capodecina
1L Soldier

KNOWN CRIMINALS

2A Top Ten or I.O. Fugitive
2B Top Thief
2C Top Con Man

FOREIGN NATIONALS

3A Legal Alien
3B Illegal Alien
3C Foreign Official W/out
Diplomatic Immunity
3D U.N. Employee W/out
Diplomatic Immunity
3E Foreign Student
3F All Others

OTHERS

8A All Other Subjects
8B Company or Corporation

TERRORISTS

4A Known Member of a
Terrorist Organization
4B Possible Terrorist Member
or Sympathizer

UNION MEMBERS

5D President
5E Vice-President
5F Treasurer
5G Secretary/Treasurer
5H Executive Board Member
5I Business Agent
5J Representative
5K Organizer
5L Business Manager
5M Financial Secretary
5N Recording Secretary
5P Office Manager
5Q Clerk
5R Shop Steward
5S Member
5T Trustee
5U Other

GOVERNMENT SUBJECTS
(6F,6G,6H- Include Agency Code)

6A Presidential Appointee
6B U.S. Senator/Staff
6C U.S. Representative/Staff
6D Federal Judge/Magistrate
6E Federal Prosecutor
6F Federal Law Enforcement Officer
6G Federal Employee - GS 13 & Above
6H Federal Employee - GS 12 & Below
6J Governor
6K Lt. Governor
6L State Legislator
6M State Judge/Magistrate
6N State Prosecutor
6P State Law Enforcement Officer
6Q State - All Others
6R Mayor
6S Local Legislator
6T Local Judge/Magistrate
6U Local Prosecutor
6V Local Law Enforcement Officer
6W Local - All Others
6X County Commissioner
6Y City Councilman

BANK EMPLOYEES

7A Bank Officer
7B Bank Employee

05/08/2003

***** COMPLAINT *****

SENSITIVE / UNCLASSIFIED

b7C

Case Number: 288A-SF-133411
Serial No.: 62

Stat Agent Name: [REDACTED]
Stat Agent SOC: [REDACTED]

Report Date: 05/08/2003
Accom Date.: 04/14/2003

Does Accomplishment Involve	Assisting Joint Agencies	Assisting Agents SOC	Subject Name
Drugs : N	CITY	[REDACTED]	GOOGLE
A Fugitive. : N			
Bankruptcy Fraud. : N			
Computer Fraud/Abuse. : Y			RA Squad Task Force
Corruption of Public Officials: N			-----
Money Laundering. : N			HRA 14B

Sub. Invest. Asst by Other FOs: BA

1 = Used, but did not help
2 = Helped, Minimally
3 = Helped, Substantially
4 = Absolutely Essential

Investigative Assistance or Technique Used

FINAN ANALYST	LAB DIV EXAMS	UCO-GROUP I	FT. MON-NRCSC
AIRCRAFT ASST	LAB FIELD SUP	UCO-GROUP II	FOR LANG ASST
COMPUTER ASST	PEN REGISTERS	UCO-OTHER	NON FBI LAB EX
CONSEN MONITR	PHOTO COVERGE	NCAVC/VI-CAP	VICT-WITN COOR
ELSUR/FISC	POLYGRAPH	CRIM/NS INTEL	IO WANTED FLYR
ELSUR/III	SRCH WAR EXEC	CRIS NEG-FED	SARS
ENG FIELD SUP	SHOW MONEY	CRIS NEG-LOC	CART
ENG TAPE EXAM	SOG ASST	ERT ASST	ASSET FORF PRO
LEGATS ASST.	SWAT TEAM	BUTTE-ITC	FORF SUPPORT P
EVIDNCE PURCH	TECH AG/EQUIP	SAVANNAH-ITC	
INFORMANT/CW	TEL TOLL RECS	POC-WRCSC	

b7E

Complaint is for Federal/Local/International (F/L/I)... : L

Civil Rico Complaint (Y/N)..... : N

United States Code Violation

Title	Section	Counts
-----	-----	-----

Accomplishment Narrative

SENSITIVE / UNCLASSIFIED

Task Force
Assisting Agencies x •
1. DSP
2.

<p>J. Civil Rico Matters Date: _____</p> <p>Also Complete "Section G"</p> <p>Other Civil Matters Date: _____</p> <p>Judgment _____ •</p> <p>Judicial Outcome _____ •x</p> <p>Amount \$ _____</p> <p>Suspension: Years _____ Months _____</p>	<p>K. Administrative Sanction Date: _____</p> <p>Subject Description Code _____ •</p> <p>Type: _____ Length: _____</p> <p><input type="checkbox"/> Suspension <input type="checkbox"/> Permanent</p> <p><input type="checkbox"/> Debarment or</p> <p><input type="checkbox"/> Injunction Year _____ Months _____</p>
<p>L. Asset Seizure Date: _____</p> <p>Asset Forfeiture Date: _____</p> <p>CATS # Mandatory _____</p> <p>Check one of the three:</p> <p><input type="checkbox"/> Asset Forfeiture - Administrative</p> <p><input type="checkbox"/> Asset Forfeiture - Civil Judicial</p> <p><input type="checkbox"/> Asset Forfeiture - Criminal</p> <p>Do not indicate \$ value in Section D</p>	
<p>M. Acquittal / Dismissal / Pretrial Diversion</p> <p>Acquittal Date: _____</p> <p>Dismissal Date: _____</p> <p>Pretrial Diversion Date: _____</p>	

☒ Additional information may be added by attaching another form or a plain sheet of paper for additional entries.
☐ See codes on reverse side.
☒ Requires that an explanation be attached and loaded into ISRAA for recovery over \$1m and PELP over \$5m.

For Further Instructions See: MAOP, Part 3, Sections 3-5 thru 3-5.3.

PROPERTY CODES

01 Cash
02 Stocks, Bonds or Negot. Instruments
03 General Retail Merchandise
04 Vehicles
05 Heavy Machinery & Equipment
06 Aircraft
07 Jewelry
08 Vessels
09 Art, Antiques or Rare Collections
11 Real Property
20 All Other

SENTENCE TYPES

CP Capital Punishment
JS Jail Sentence
LP Life Parole
LS Life Sentence
NS No Sentence (Subject is a Fugitive,
Insane, has Died, or is a
Corporation)
PB Probation
SJ Suspension of Jail Sentence
YC Youth Correction Act

PELP CODES

22 Counterfeit
Stocks/Bonds/Currency/
Negotiable Instruments
23 Counterfeit/Pirated Sound
Recordings or Motion Pictures
24 Bank Theft Scheme Aborted
25 Ransom, Extortion or Bribe
Demand Aborted
26 Theft From or Fraud Against
Government Scheme Aborted
27 Commercial or Industrial
Theft Scheme Aborted
30 All Other

ORGANIZED CRIME SUBJECTS

1F Boss
1G Underboss
1H Consigliere
1I Acting Boss
1K Capodecina
1L Soldier

KNOWN CRIMINALS

2A Top Ten or I.O. Fugitive
2B Top Thief
2C Top Con Man

FOREIGN NATIONALS

3A Legal Alien
3B Illegal Alien
3C Foreign Official W/out
Diplomatic Immunity
3D U.N. Employee W/out
Diplomatic Immunity
3E Foreign Student
3F All Others

OTHERS

8A All Other Subjects
8B Company or Corporation

RACE CODES

A Asian/Pacific Islander
B Black
I Indian/American
U Unknown
W White
X Nonindividual

AGENCY CODES

AFOIS Air Force Office of Special Investigations
ACIS Army Criminal Investigative Service
BATF Bureau of Alcohol, Tobacco & Firearms
BIA Bureau of Indian Affairs
DCAA Defense Contract Audit Agency
DCIS Defense Criminal Investigative Service
DEA Drug Enforcement Administration
DOC Department of Corrections
DOI Dept. of Interior
EPA Environmental Protection Agency
FAA Federal Aviation Administration
FDA Food and Drug Administration
HHS Dept. of Health & Human Services
HUD Dept. of Housing & Urban Development
INS Immigration and Naturalization Service
IRS Internal Revenue Service
NASA Nat'l Aeronautics & Space Admin
NBIS Nat'l NARC Border Interdiction
NCIS Naval Criminal Investigative Service
RCMP Royal Canadian Mounted Police
SBA Small Business Administration
USBP U.S. Border Patrol
USCG U.S. Coast Guard
USCS U.S. Customs Service
USDS U.S. Department of State
USMS U.S. Marshals Service
USPS U.S. Postal Service
USSS U.S. Secret Service
USTR U.S. Treasury
LOC Local
CITY City
COUN County
ST State
OTHR Other

SUBJECT DESCRIPTION CODES

TERRORISTS

4A Known Member of a
Terrorist Organization
4B Possible Terrorist Member
or Sympathizer

UNION MEMBERS

5D President
5E Vice-President
5F Treasurer
5G Secretary/Treasurer
5H Executive Board Member
5I Business Agent
5J Representative
5K Organizer
5L Business Manager
5M Financial Secretary
5N Recording Secretary
5P Office Manager
5Q Clerk
5R Shop Steward
5S Member
5T Trustee
5U Other

JUDGMENT CODES

CJ Consent Judgment
CO Court Ordered Settlement
DF Default Judgment
DI Dismissal
JN Judgment Notwithstanding
MV Mixed Verdict
SJ Summary Judgment
VD Verdict for Defendant
VP Verdict for Plaintiff

JUDICIAL OUTCOME

AG Agreement
BR Barred/Removed
CC Civil Contempt
DC Disciplinary Charges
FI Fine
PI Preliminary Injunction
PR Temporary Restraining Order
PS Pre-filing Settlement
RN Restitution
SP Suspension
VR Voluntary Resignation
OT Other

SUBJECT PRIORITY

A Subject wanted for crimes of violence
(i.e., murder, manslaughter, forcible
rape) against another individual or
convicted of such a crime in the past five
years
B Subject wanted for crimes involving loss
or destruction of property valued in
excess of \$25,000 or convicted of such a
crime in the past five years.
C All other subjects.

GOVERNMENT SUBJECTS (6F,6G,6H- Include Agency Code)

6A Presidential Appointee
6B U.S. Senator/Staff
6C U.S. Representative/Staff
6D Federal Judge/Magistrate
6E Federal Prosecutor
6F Federal Law Enforcement Officer
6G Federal Employee - GS 13 & Above
6H Federal Employee - GS 12 & Below
6J Governor
6K Lt. Governor
6L State Legislator
6M State Judge/Magistrate
6N State Prosecutor
6P State Law Enforcement Officer
6Q State - All Others
6R Mayor
6S Local Legislator
6T Local Judge/Magistrate
6U Local Prosecutor
6V Local Law Enforcement Officer
6W Local - All Others
6X County Commissioner
6Y City Councilman

BANK EMPLOYEES

7A Bank Officer
7B Bank Employee

11/22/81 - 12/2/81

04/24/2003

***** COMPLAINT *****

SENSITIVE / UNCLASSIFIED

b7C

Case Number: 288A-SF-133411

Stat Agent Name:

Report Date: 04/24/2003

Serial No.:

Stat Agent SOC.:

Accom Date.: 04/14/2003

Does Accomplishment Involve

Assisting Joint Agencies

Assisting Agents SOC

Subject Name

Drugs : N
A Fugitive. : N
Bankruptcy Fraud. : N
Computer Fraud/Abuse. : Y
Corruption of Public Officials: N
Money Laundering. : N

ST

b7C
b3

RA Squad Task Force

DOVE 17

Sub. Invest. Asst by Other FOs:

1 = Used, but did not help
2 = Helped, Minimally
3 = Helped, Substantially
4 = Absolutely Essential

Investigative Assistance or Technique Used

FINAN ANALYST	LAB DIV EXAMS	UCO-GROUP I	FT. MON-NRCSC
AIRCRAFT ASST	LAB FIELD SUP	UCO-GROUP II	FOR LANG ASST
COMPUTER ASST	PEN REGISTERS	UCO-OTHER	NON FBI LAB EX
CONSEN MONITR	PHOTO COVERGE	NCAVC/VI-CAP	VICT-WITN COOR
ELSUR/FISC	POLYGRAPH	CRIM/NS INTEL	IO WANTED FLYR
ELSUR/III	SRCH WAR EXEC	CRIS NEG-FED	SARS
ENG FIELD SUP	SHOW MONEY	CRIS NEG-LOC	CART
ENG TAPE EXAM	SOG ASST	ERT ASST	ASSET FORF PRO
LEGATS ASST.	SWAT TEAM	BUTTE-ITC	FORF SUPPORT P
EVIDNCE PURCH	TECH AG/EQUIP	SAVANNAH-ITC	
INFORMANT/CW	TEL TOLL RECS	POC-WRCSC	

Complaint is for Federal/Local/International (F/L/I)... : L

Civil Rico Complaint (Y/N)..... : N

United States Code Violation

Title Section Counts

Accomplishment Narrative

SENSITIVE / UNCLASSIFIED

Accomplishment Report

(Accomplishment must be reported and loaded into ISRAA within 30 days from date of accomplishment)

Date Prepared 4-21-93

Date Loaded: 4-24-03

Data Loader's Initials AW

Accomplishment involves: (check all that apply)	
Drugs	<input type="checkbox"/>
A Fugitive	<input type="checkbox"/>
Bankruptcy Fraud	<input type="checkbox"/>
Computer Fraud/Abuse	<input type="checkbox"/>
Corruption of Public Officials	<input type="checkbox"/>
Money Laundering	<input type="checkbox"/>
Sub Invest Asst by FO (s)	<input type="checkbox"/>

File Number
288A-SF-133411

Stat Agent Soc. Sec. No.Stat Agent Name

RA	Squad
DOVER	17

Asst. FO(s) SE, , ,
A. B. C. D

Task Force

Assisting Agencies x ●
1. DSP
2.

Assisting Agents Soc. Sec. No. ^x

1. - -

Name: _____

2. - -

Name: _____

Investigative Assistance or Technique Used											
1-Used, but did not help				3 - Helped, substantially							
2 -Helped, minimally				4 - Absolutely essential							
For Sub. Invest. Assist. by other FO (s) indicate A,B,C,D for corresponding FO											
Rate	FO	IAT	Rate	FO	IAT	Rate	FO	IAT	Rate	FO	IAT
		Fin. Analyst			Lab. Div. Exam			UCO - Group I			Ft. Mon.- ITC
		Aircraft Asst.			Lab. Field Sup			UCO - Group II			For. Lang Asst.
		Computer			Pen Registers			UCO - Nat. Back			Non FBI Lab Ex
		Consen Mon.			Photo Cover.			NCAVC / VI - CAP			Vict-With Coor
		Elsur / FISC			Polygraph			Crim/NS Intel Asst			IO Wanted Flye
		Elsur / T. III			Search Warrant			Crisis Neg. - Fed.			SARs
		Eng. Field Spt.			Show Money			Crisis Neg. - Local			CART
		Eng. Tape Ex			SOG Asst.			ERT Asst.			
		Legats Asst.			Swat Team			Butte - ITC			
		Evid Purchase			Tech. Ag/Equip.			Sav - ITC			
		Int/CW Info			Phone Toll Rec			Poc - ITC			

A. Complaint / Information / Indictment
☐ Federal ☐ Local ☐ International
Complaint Date: _____
 Check if Civil Rico Complaint ☐
Information Date: _____
Indictment Date: _____

B. Locate/Arrest

☐ Federal ☒ Local ☐ International

Subject Priority: ☐ A ☐ B ☒ C

Locate Date: _____

Arrest Date: 4-15-03

☐ Subject Resisted Arrest

☐ Subject Arrested was Armed

C. Summons Date: _____
☐ Federal ☐ Local

D. Recovery/Restitution/PELP X

☐ Federal ☐ Local ☐ International

Recovery Date: _____

Code • _____ ✓ Amount \$ _____

Code • _____ ✓ Amount \$ _____

Restitution Date: _____

☐ Court Ordered ☐ Pretrial Diversion

Code • _____ ✓ Amount \$ _____

PELP Date: _____

Code • _____ ✓ Amount \$ _____

E. Hostage(s) Released Date: _____
Released by: ☐ Terrorist ☐ Other
Number of Hostages: _____
Child Located Date: _____

F. Conviction

☐ Federal ☐ Local ☐ International

Conviction Date: _____

Subject Description Code: _____ • (_____) •

For 6F, G, H-Include Agency Code

☐ Felony or ☐ Misdemeanor

☐ Plea or ☐ Trial

State: _____ **Judicial District:** _____

G. U.S. Code Violation		
Required for sections A,B,F,and J (Federal Only)		
Title	Section	# Counts

H. Sentence Date: _____
Sentence Type: _____
In Jail: Years _____ Months _____
Suspended: Years _____ Months _____
Probation: Years _____ Months _____
Fines: \$ _____

I. Disruption/Dismantlement:
 Disruption Date: _____
 Dismantlement Date: _____
 Completion of FD-515a Side 2 Mandatory

J. Civil Rico Matters Date: _____

Also Complete "Section G"

Other Civil Matters Date: _____

Judgment _____ •

Judicial Outcome _____ •x

Amount \$ _____

Suspension: Years _____ Months _____

K. Administrative Sanction Date: _____

Subject Description Code _____ •

Type: _____ **Length:** _____

☐ Suspension ☐ Permanent

☐ Debarment or

☐ Injunction **Year** _____ **Months** _____

L. Asset Seizure Date: _____
Asset Forfeiture Date: _____
CATS # Mandatory _____

Check one of the three:

☐ Asset Forfeiture - Administrative
☐ Asset Forfeiture - Civil Judicial
☐ Asset Forfeiture - Criminal

Do not indicate \$ value in Section D

M. Acquittal / Dismissal / Pretrial Diversion

Acquittal Date: _____

Dismissal Date: _____

Pretrial Diversion Date: _____

N. Subject Information (Required for all Sections excluding Section D (Recovery/PELP), Section E (Hostage), Section I, and Section L).

Name	Page #	Sex	Date of Birth	Social Security No. (if available)
<div style="border: 1px solid black; height: 40px; width: 100%;"></div>				b7C

For indictments/convictions only.

☐ Subject related to an LCN, Asian Organized Crime (AOC), Italian Organized Crime (IOC), Russian/Eastern European, Caribbean, or Nigerian Organized Crime Group - Complete FD-515a, Side 1 Blocks A-E mandatory, F-H as appropriate. b3

☐ Subject related to an OC/Drug Organization, a VCMO Program National Gang Strategy target group, or a VCMO Program National Priority Initiative target group - Complete FD-515a, Side 1 Blocks A-C only.

- ✕ Additional information may be added by attaching another form or a plain sheet of paper for additional entries.
- See codes on reverse side.
- ✓ Requires that an explanation be attached and loaded into ISRAA for recovery over \$1m and PELP over \$5m.

Serial No. of FD-515

288A-SF-133411

For Further Instructions See: MAOP, Part 2, Sections 3-5 thru 3-5.3.

PROPERTY CODES

01 Cash
02 Stocks, Bonds or Negot. Instruments
03 General Retail Merchandise
04 Vehicles
05 Heavy Machinery & Equipment
06 Aircraft
07 Jewelry
08 Vessels
09 Art, Antiques or Rare Collections
11 Real Property
20 All Other

SENTENCE TYPES

CP Capital Punishment
JS Jail Sentence
LP Life Parole
LS Life Sentence
NS No Sentence (Subject is a Fugitive,
Insane, has Died, or is a
Corporation)
PB Probation
SJ Suspension of Jail Sentence
YC Youth Correction Act

PELP CODES

22 Counterfeit
Stocks/Bonds/Currency/
Negotiable Instruments
23 Counterfeit/Pirated Sound
Recordings or Motion Pictures
24 Bank Theft Scheme Aborted
25 Ransom, Extortion or Bribe
Demand Aborted
26 Theft From or Fraud Against
Government Scheme Aborted
27 Commercial or Industrial
Theft Scheme Aborted
30 All Other

RACE CODES

A Asian/Pacific Islander
B Black
I Indian/American
U Unknown
W White
X Nonindividual

AGENCY CODES

AFOIS Air Force Office of Special Investigations
ACIS Army Criminal Investigative Service
BATF Bureau of Alcohol, Tobacco & Firearms
BIA Bureau of Indian Affairs
DCAA Defense Contract Audit Agency
DCIS Defense Criminal Investigative Service
DEA Drug Enforcement Administration
DOC Department of Corrections
DOI Dept. of Interior
EPA Environmental Protection Agency
FAA Federal Aviation Administration
FDA Food and Drug Administration
HHS Dept. of Health & Human Services
HUD Dept. of Housing & Urban Development
INS Immigration and Naturalization Service
IRS Internal Revenue Service
NASA Nat'l Aeronautics & Space Admin
NBIS Nat'l NARC Border Interdiction
NCIS Naval Criminal Investigative Service
RCMP Royal Canadian Mounted Police
SBA Small Business Administration
USBP U.S. Border Patrol
USCG U.S. Coast Guard
USCS U.S. Customs Service
USDS U.S. Department of State
USMS U.S. Marshals Service
USPS U.S. Postal Service
USSS U.S. Secret Service
USTR U.S. Treasury
LOC Local
CITY City
COUN County
ST State
OTHR Other

JUDGMENT CODES

CJ Consent Judgment
CO Court Ordered Settlement
DF Default Judgment
DI Dismissal
JN Judgment Notwithstanding
MV Mixed Verdict
SJ Summary Judgment
VD Verdict for Defendant
VP Verdict for Plaintiff

JUDICIAL OUTCOME

AG Agreement
BR Barred/Removed
CC Civil Contempt
DC Disciplinary Charges
FI Fine
PI Preliminary Injunction
PR Temporary Restraining Order
PS Pre-filing Settlement
RN Restitution
SP Suspension
VR Voluntary Resignation
OT Other

SUBJECT PRIORITY

A Subject wanted for crimes of violence
(i.e., murder, manslaughter, forcible
rape) against another individual or
convicted of such a crime in the past five
years
B Subject wanted for crimes involving loss
or destruction of property valued in
excess of \$25,000 or convicted of such a
crime in the past five years.
C All other subjects.

SUBJECT DESCRIPTION CODES

ORGANIZED CRIME
SUBJECTS

1F Boss
1G Underboss
1H Consigliere
1J Acting Boss
1K Capodecina
1L Soldier

KNOWN CRIMINALS

2A Top Ten or I.O. Fugitive
2B Top Thief
2C Top Con Man

FOREIGN NATIONALS

3A Legal Alien
3B Illegal Alien
3C Foreign Official W/out
Diplomatic Immunity
3D U.N. Employee W/out
Diplomatic Immunity
3E Foreign Student
3F All Others

OTHERS

8A All Other Subjects
8B Company or Corporation

TERRORISTS

4A Known Member of a
Terrorist Organization
4B Possible Terrorist Member
or Sympathizer

UNION MEMBERS

5D President
5E Vice-President
5F Treasurer
5G Secretary/Treasurer
5H Executive Board Member
5I Business Agent
5J Representative
5K Organizer
5L Business Manager
5M Financial Secretary
5N Recording Secretary
5P Office Manager
5Q Clerk
5R Shop Steward
5S Member
5T Trustee
5U Other

GOVERNMENT SUBJECTS
(6F,6G,6H- Include Agency Code)

6A Presidential Appointee
6B U.S. Senator/Staff
6C U.S. Representative/Staff
6D Federal Judge/Magistrate
6E Federal Prosecutor,
6F Federal Law Enforcement Officer
6G Federal Employee - GS 13 & Above
6H Federal Employee - GS 12 & Below
6J Governor
6K Lt. Governor
6L State Legislator
6M State Judge/Magistrate
6N State Prosecutor
6P State Law Enforcement Officer
6Q State - All Others
6R Mayor
6S Local Legislator
6T Local Judge/Magistrate
6U Local Prosecutor
6V Local Law Enforcement Officer
6W Local - All Others
6X County Commissioner
6Y City Councilman

BANK EMPLOYEES

7A Bank Officer
7B Bank Employee

04/24/2003

***** ARREST *****
SENSITIVE / UNCLASSIFIED b7C

Case Number: 288A-SF-133411 Stat Agent Name: [Redacted] Report Date: 04/24/2003
Serial No.: Stat Agent SOC: [Redacted] Accom Date.: 04/15/2003

Does Accomplishment Involve	Assisting Joint Agencies	Assisting Agents SOC	Subject Name
Drugs : N	ST	b7C	[Redacted]
A Fugitive. : N			
Bankruptcy Fraud. : N		b3	
Computer Fraud/Abuse. : Y			RA Squad Task Force
Corruption of Public Officials: N			-----
Money Laundering. : N			DOVE 17

Sub. Invest. Asst by Other FOs: 1 = Used, but did not help
Investigative Assistance or Technique Used 2 = Helped, Minimally
----- 3 = Helped, Substantially
----- 4 = Absolutely Essential

FINAN ANALYST	LAB DIV EXAMS	UCO-GROUP I	FT. MON-NRCSC
AIRCRAFT ASST	LAB FIELD SUP	UCO-GROUP II	FOR LANG ASST
COMPUTER ASST	PEN REGISTERS	UCO-OTHER	NON FBI LAB EX
CONSEN MONITR	PHOTO COVERGE	NCAVC/VI-CAP	VICT-WITN COOR
ELSUR/FISC	POLYGRAPH	CRIM/NS INTEL	IO WANTED FLYR
ELSUR/III	SRCH WAR EXEC	CRIS NEG-FED	SARS
ENG FIELD SUP	SHOW MONEY	CRIS NEG-LOC	CART
ENG TAPE EXAM	SOG ASST	ERT ASST	ASSET FORF PRO
LEGATS ASST.	SWAT TEAM	BUTTE-ITC	FORF SUPPORT P
EVIDNCE PURCH	TECH AG/EQUIP	SAVANNAH-ITC	
INFORMANT/CW	TEL TOLL RECS	POC-WRCSC	

Arrest is for Federal, Local, or International (F/L/I).. : L
Arrest Subject Priority (A/B/C)..... : C
Did Subject Resist (Y/N)..... : N
Was Subject Armed (Y/N)..... : N

United States Code Violation

Title	Section	Count
-----	-----	-----

Accomplishment Narrative

FEDERAL BUREAU OF INVESTIGATION

Precedence: ROUTINE

Date: 05/09/2003

To: Baltimore

Attn: SA [REDACTED]

From: San Francisco

14B/Hayward

Contact: SA [REDACTED]

b7C

Approved By: [REDACTED] PTT/AUB

Drafted By: [REDACTED] am

Case ID #: 288A-SF-133411 - 65 (Pending)

Title: [REDACTED]

b7C

GOOGLE - VICTIM
SUNNYVALE, CA
NIPC - Impairment
01/02/2003

b3

Synopsis: To set lead to Baltimore requesting assistance in obtaining a search warrant.

Administrative: A previous request was made on February 25, 2003, for assistance in executing a search warrant. The February 25, 2003, request was obliged by the issuance of a state search warrant, executed by the Delaware State Police. This search warrant request is for obtaining a search warrant for the seized items, currently in possession of the Delaware State Police.

Enclosure(s): One (1) hard copy and one (1) soft copy of the above mentioned search affidavit and associated attachments (A and B) are provided.

Details: Google.com was a victim of two Denial of Service (DOS) attacks on January 2, 2003. The first attack occurred around 4:00 A.M. PST, lasting approximately five to seven minutes, and affected Google.com's Santa Clara servers. The second attack occurred around 3:00 P.M. PST, lasting approximately five to seven minutes, and affected both Google.com's Santa Clara and Virginia servers. The first attack was a DOS attack comprised of both UDP and Ping Flood attacks. The second attack was on a much larger scale and consisted of a SYN Flood attack.

Investigation has led to the identification of [REDACTED] as the subject. [REDACTED] is responsible for several computer intrusions and Denial of Service (DOS) attacks. [REDACTED] commits the DOS attacks by [REDACTED]

b7C

b3

b7C

✓ c: [REDACTED] /SEARCH.EC

288A-SF-133411-65

To: Baltimore From: San Francisco
Re: 288A-SF-133411, 05/09/2003

b2

The property to be searched is currently in possession of the Delaware State Police, 1575 McKee, Dover, Delaware, 19904. The Delaware State Police have agreed to duplicate the seized computers and computer systems of [redacted] detailed in the attached search affidavit.

b7C

b3

San Francisco Division requests the assistance of Baltimore Division, Dover Resident Agency, in obtaining a search warrant for the above referenced property.

To: Baltimore From: San Francisco
Re: 288A-SF-133411, 05/09/2003

LEAD(s) :

Set Lead 1:

BALTIMORE

AT DELAWARE

b7C

Please provide assistance in obtaining a search warrant for the computers and computer systems of Documentation, including the search affidavit and associated attachments, is enclosed.

b7C

b3

♦♦

- 1 -

FEDERAL BUREAU OF INVESTIGATION

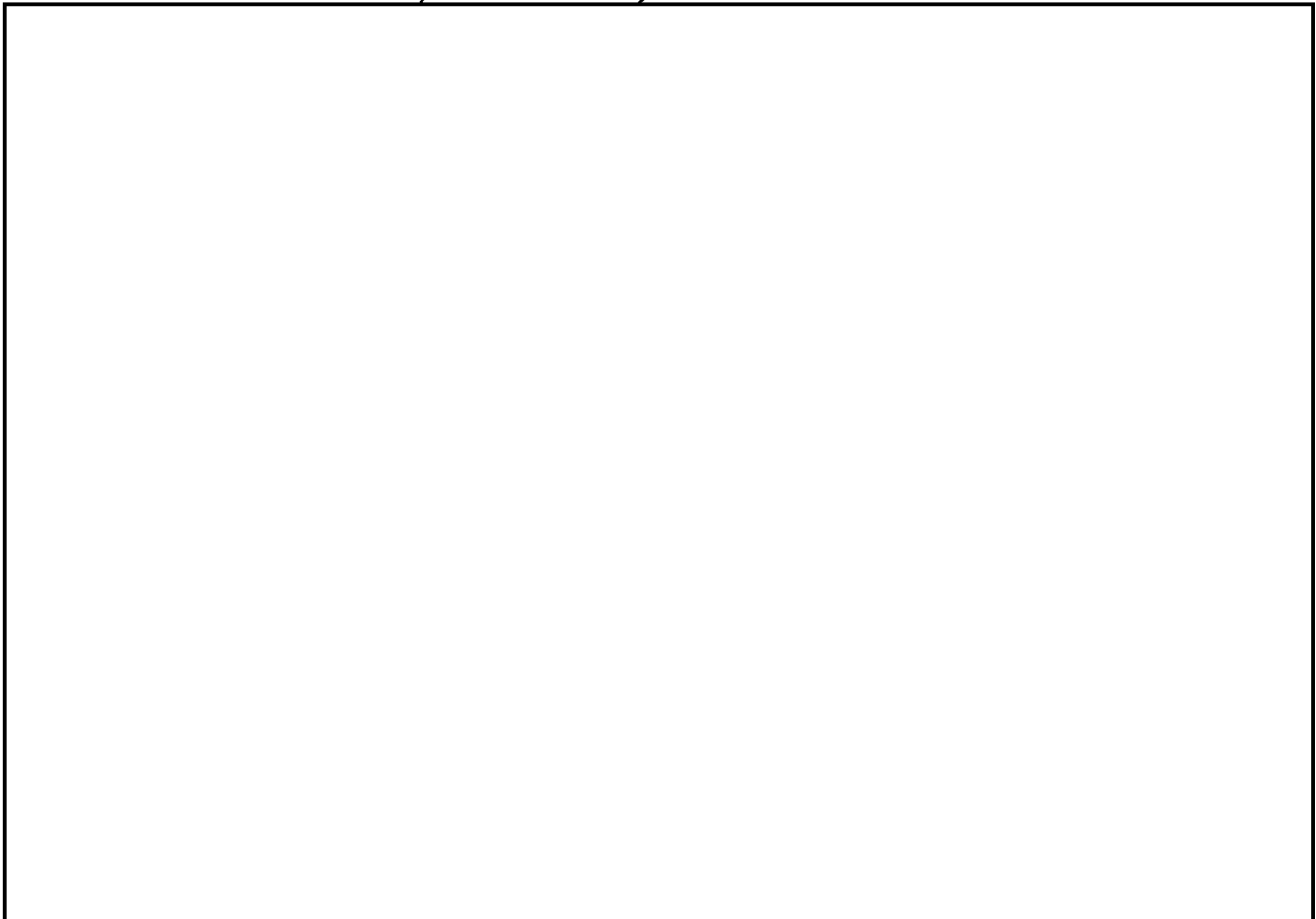
Date of transcription 04/28/2003

b7C

SOURCE, who is not in a position to testify, was in contact with SA [redacted] on 04/25/2003. SOURCE provided the Internet relay chat (IRC) log information provided below of connections for the nickname [redacted] to the IRC network [redacted] channel [redacted]. All times are in GMT. SOURCE believes that [redacted] is an individual, and that the other nicknames listed are IRC robot programs (bots).

b2

MOH



b2

b7C

Investigation on 04/28/2003 at Chicago, Illinois

b2

File # 288A-SF-133411, [redacted]Date dictated 04/28/2003

b7D

by SA [redacted]

b7C

This document contains neither recommendations nor conclusions of the FBI. It is the property of the FBI and is loaned to your agency; it and its contents are not to be distributed outside your agency.

118mdh01.302

M 5/20/03

AM 2

FEDERAL BUREAU OF INVESTIGATION

Precedence: ROUTINE

Date: 05/27/2003

To: San Francisco

Attn: SA [REDACTED]

From: San Francisco

Squad 14B, San Jose RA, CART

Contact: [REDACTED]

b7C

Approved By: [REDACTED] W

Drafted By: [REDACTED]

bcl BCL

Case ID #: 196E-SF-133411

(Pending) - 68 b2

288A-SF-129533

(Pending)

b7D

[REDACTED] (Pending)

Title: [REDACTED]

b7C

GOOGLE - VICTIM;

SUNNYVALE, CA

b3

NIPC - IMPAIRMENT

Synopsis: Access to Internet proxy enabled.

Reference: 196E-SF-133411 Serial 50

Details: On May 27, 2003, the following user name and password were created for SA [REDACTED] for the above captioned case.

b7C

The user name and password is unique for this case and reports will be generated quarterly for case activity, and forwarded to the case agent.

User: [REDACTED]

b7C

Password: [REDACTED]

b2

Above referenced lead is considered covered.

♦♦
i:

[REDACTED]

\20030527-2.ec

b7C

288-SF-133411-68

- 1 -

FEDERAL BUREAU OF INVESTIGATION

Date of transcription 04/22/2003

On April 17, 2003, source who is not in the position to testify was electronically contacted via e-mail by SA [redacted] b7C
 [redacted] The e-mail was received and a response was received by SA [redacted] on April 22, 2003. The body of the April 22, 2003 e-mail received by SA [redacted] and SA [redacted] April 17, 2003 e-mail contained the following:

 Hey [redacted]

I've been keeping an eye out all weekend and I don't see anyone at all.

everyone scrambled like flies. if [redacted] did come on I think he would be hiding well. but I will keep an eye out for [redacted]

do you know [redacted] nick/handle? I'm not familiar with that name.

also; a lot of the members from [redacted] hang out in [redacted] I've been watching that channel too.

* Now talking in [redacted]

* ChanServ sets mode [redacted]

* ChanServ changes topic to 'don't even think of joining this channel again'

-NickServ- Info for [redacted]

-NickServ- Last seen address : [redacted]

-NickServ- Last seen time : Fri 04/11/2003 6:01:33pm GMT

-NickServ- Time registered : Thu 10/24/2002 2:56:38am GMT

-NickServ- Expiration time: Sun May 11 11:01:46am 2003 (local time)

-NickServ- Expires in: 2wks 5days 18hrs 34mins 21secs

-NickServ- Time now : Mon 04/21/2003 23:27:12 GMT

From: "SA [redacted]" - San Francisco FBI [redacted]

To: [redacted]

Subject: [redacted]

Date: Thu, 17 Apr 2003 16:55:39 -0700

Investigation on 04/22/2003 at Hayward, CA

File [redacted] 288A-SF-133444-4 Date dictated Not Dictated

by SA [redacted]

[Redacted]

288A-SF-133441

b2

b7D

Continuation of FD-302 of

[Redacted]

, On 04/22/2003

, Page 2

Hey

[Redacted]

[Redacted]

[Redacted]

Can you check out [Redacted] (or

b7D

any other location) and see if he goes on-line? He's got a buddy
accomplished hacker; Heard of him? Can you keep an eye out?

[Redacted]

who's supposedly an

b3

b7C

Thanks,

[Redacted]

b7C

FEDERAL BUREAU OF INVESTIGATION

Precedence: ROUTINE

Date: 06/23/2003

To: San Francisco

From: San Francisco

14B/Hayward

Contact: SA [REDACTED]

Approved By: [REDACTED]

b7C

Drafted By: [REDACTED]

am *Am*

Case ID #: 288A-SF-133411 (Pending)

Title: [REDACTED]

GOOGLE-VICTIM

SUNNYVALE, CA

NIPC-IMPAIRMENT

b7C

b3

Synopsis: San Francisco requests the closing of the above captioned case.

Details: Google.com was a victim of two Denial of Service (DOS) attacks on January 2, 2003. The first attack occurred around 4:00 A.M. PST, lasting approximately five to seven minutes, and affected Google.com's Santa Clara servers. The second attack occurred around 3:00 P.M. PST, lasting approximately five to seven minutes, and affected both Google.com's Santa Clara and Virginia servers. The first attack was a DOS attack comprised of both UDP and Ping Flood attacks. The second attack was on a much larger scale and consisted of a SYN Flood attack.

Investigation has led to the identification of [REDACTED] as the subject. [REDACTED] is responsible for several computer intrusions and Denial of Service (DOS) attacks. [REDACTED] commits the DOS attacks by [REDACTED]

b7C

b3

b2

On June 9, 2003, [REDACTED]

1/8/03
Rotor
P10 close
case
c=4
m
6/24/03

b7C

C: [REDACTED]

133411 01. EC

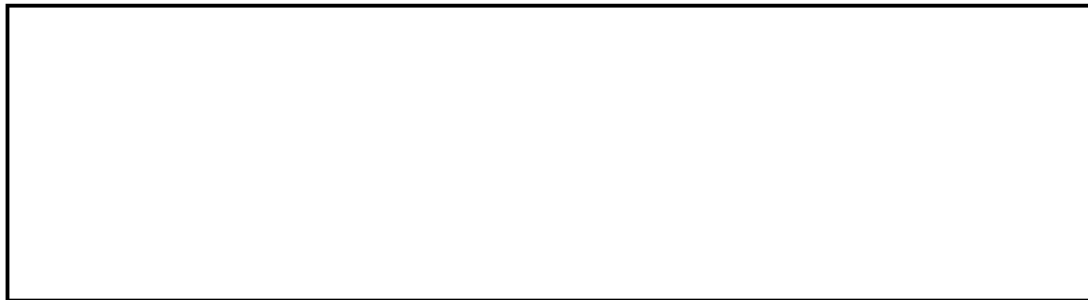
288A-SF-133411-71

CASE NOT
closed due to
outstanding (CAs)

To: San Francisco From: San Francisco
Re: 288A-SF-133411, 06/23/2003

b3 18 USC 5038

b7C



San Francisco holds no evidence in above captioned case. San Francisco request that, due to successful local prosecution of [redacted] that the case be closed.

b7C

♦♦